UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

- - - - -

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No. 1:16CR224
	)	
BOGDAN NICOLESCU,	)	
RADU MICLAUS,	)	
	)	
Defendants.	)	

- - - - -

CONTINUED TRANSCRIPT OF TRIAL PROCEEDINGS HAD

BEFORE HONORABLE JUDGE PATRICIA A. GAUGHAN, JUDGE

OF SAID COURT, ON THURSDAY, APRIL 4TH, 2019,

COMMENCING AT 9:00 O'CLOCK A.M.

- - - - -

Volume 9, Pages 1584 through 1792

- - - - -

Court Reporter: GEORGE J. STAIDUHAR
801 W. SUPERIOR AVE.,
SUITE 7-184
CLEVELAND, OHIO 44113
(216) 357-7128

APPEARANCES:

On behalf of the Government:

OFFICE OF THE U.S. ATTORNEY
BY: DUNCAN T. BROWN, AUSA
BRIAN M. McDONOUGH, AUSA
801 West Superior Ave., Suite 400
Cleveland, OH 44113

and

U.S. DEPARTMENT OF JUSTICE - CRIMINAL DIVISION
BY: BRIAN L. LEVINE, SENIOR COUNSEL
1301 New York Avenue, Suite 600
Washington, DC 20530

On behalf of Defendant Bogdan Nicolescu:

LAW OFFICE OF MICHAEL J. GOLDBERG
BY: MICHAEL J. GOLDBERG, ESQ.
323 Lakeside Place, Suite 450
Cleveland, OH 44113

On behalf of Defendant Radu Miclaus:

LIPSON O'SHEA
BY: MICHAEL J. O'SHEA, ESQ.
110 Hoyt Block Building
700 West St. Clair Avenue
Cleveland, OH 44113

- - - - -

I N D E X

P R O C E E D I N G S

THE COURT: Please be seated, ladies and gentlemen. Good morning.

You may continue, Mr. Brown.

MR. BROWN: Thank you.

RYAN MACFARLANE

resumed the witness stand by and on behalf of the Government, being previously sworn, was examined and testified further as follows:

DIRECT EXAMINATION CONTINUED

BY MR. BROWN:

Q. Special Agent Macfarlane, I believe when we stopped yesterday we were talking about items you found during your search of the data on the command and control servers. Do you recall that?

A. I do, yes.

Q. And I believe we left off when you were talking about the organization of data as related to the auto auction fraud, correct?

A. Yes. I believe that is also correct.

Q. Did you also see similar data tables concerning the information harvested from victims.

A. Yes. On the command and control server, there was a large database that contained over 52 different tables on the first server that we did the search warrant on, and

those tables contained, if my memory serves me correctly, five to six tables related to auto auction fraud, a table related to credit card information, tables related to mule tables, related to infected systems tables, tables related to spam, tables related to the collection of account credentials and other tables that were supporting different aspects of the Bayrob botnet.

Q. And without publishing to the jury I would like to show you exhibit 1204. Do you recognize this?

A. Yes, I do.

Q. How do you recognize this?

A. So this is the data that was contained in the table CC on one of the command and control servers in the database?

So the database would contain many different tables, and this was one of those tables.

Q. Did you create this data?

A. No.

Q. Did you modify this data?

A. Yes.

Q. How did you --

A. I mean, no. No, I didn't modify it.

Q. Did you format this data?

A. I pulled this data out of the database into this format, yes.

Q. Did you use a program to pull that data out.
A. I did, yes.
Q. Did that change any of the data?
A. No.
Q. Did it — did exporting that data using your program allow you to put it into a readable format?
A. Yes.
Q. Or a format that you could analyze?
A. Yes.
Q. Is this a fair and accurate representation of the data you found on the command and control server concerning a CC table?
A. Yes.

MR. BROWN: Your Honor, permission to publish to the jury?

MR. GOLDBERG: No objection.

MR. O'SHEA: No objection.

MR. BROWN: Thank you.

BY MR. BROWN:
Q. Special Agent Macfarlane, could you explain what this table shows?
A. Sure. Starting at column 1 would be the row identifier for each row within this table.
Q. Okay. And what does the next column mean to you based on your investigation?

A. My assessment of this column means that this card is no longer good. If it was good, there would be a 1. If it is no longer good, it would be a zero.
Q. And column 3, what is that information, what does that mean to you, if anything?
A. That column contains notes by members of the Bayrob Group.
Q. And did you enter any of that information?
A. I did not.
Q. And approximately how long is this exhibit?
A. I need to see it.
Q. Could you zoom out?
A. On the bottom there, it says page 1 of 10, but I don't know if we — I could review the exhibit in person, but based on that, I assume it is ten pages.
Q. Do you recall some of the names you saw in the names column?
A. Yes.
Q. Could you zoom in just on the names column, the notes column? Could you read some of the names you saw?
A. Minolta, national at this he anyway, Keke.
Q. And what are some of the other notes in addition to names or monikers?
A. Some of the other notes are services that were used

by the Bayrob Group such as Yahoo host, for example.
Q. And do those notes have any importance to you based on your investigation?
A. Yes. So those notes would indicate what that credit card was used for. Example, in this row down here, you can see the note "dream host VPS and "Yahoo host."
That would indicate that that credit card was used both for hosting a dream host and then for a domain at Yahoo hosting.
Q. And could you zoom out, please? And then, the next column is entitled "name." Is that correct?
A. Yes.
Q. And what does that column mean to you, if anything?
A. That would be the name of the person on the credit card.
Q. And the next column is an address?
A. Yes.
Q. The next two are addresses, correct?
A. Yes.
Q. And what did those mean to you, if anything, in this investigation?
A. Those would be the addresses related to that credit card.
Q. Okay. Same with city and states?

A. Yes.
Q. Using the names and addresses, cities, state columns, what, if anything, were you able to do to further your investigation with that information?
A. We were able to speak with some of the individuals on this list and notify victims that their credit cards were stolen based on this table.
Q. Looking towards the right of that table, what is the CC column based on your investigation?
A. That would be the credit card number.
Q. And what are the four columns to the right of that?
A. Those would be the expiration and then CBB that you would find on the back of the card.
Q. And based on your investigation, why was it important to have those three columns as well as the numbers?
A. Because that's what you need to use for the credit card.
Q. And now, Special Agent Macfarlane, looking at this table, in fact, was there something that was changed during the formatting process concerning this data?
A. Yes. Yes, there was.
Q. Could you explain to the jury what that was?

A. So the CC row, when you put a 16-digit number into Excel, Excel only supports what's called a 15-digit floating number?

And during the export process and providing this into the trial format, when it was loaded up in Excel, if you don't do it in a specific way, it will basically round the last number incorrectly.

So for example, when you see CC 807090, the underlying data actually has a different digit, which is specific to the credit card.

Q. When you talked to victims, did you rely on this credit card number or the credit card number in the underlying data?

A. The underlying data.

Q. And were you able to confirm with the victims you spoke with that that underlying -- that the credit card number in the underlying data was, in fact, the correct -- or their credit card?

A. Yes.

MR. GOLDBERG: Objection.

THE COURT: Overruled.

A. Yes. And we would confirm other aspects such as phone numbers and addresses. When possible, we would get credit card statements.

Q. And in fact, did you see the name Lynn Stallings on

this list?
A. Yes. It was in one of these tables.
Q. Did you confirm that a Lynn Stallings' information as it was on the database was, in fact, her information?
A. Yes.
Q. Including her credit card?
A. Yes.
Q. Did you — do you recall speaking with a Clinton Berke?
A. Yes.
Q. Was Clinton Berke on this table?
A. Yes.
Q. When you spoke with him, did you confirm his credit card information from the database was his credit card information?
A. Yes.
Q. Did you speak with Don Wertz?
A. Yes, I did.
Q. Was Don Wertz' name and credit card information on this list?
A. Yes.
Q. And when you spoke with Don Wertz, did he confirm that the credit card information from the database was his credit card information?

A. Yes.
Q. Did you speak with a Terry Muhlenkamp?
A. Yes.
Q. With Terry Muhlenkamp?
A. Actually, I don't think we talked to Terry. I think we talked to his wife maybe.
Q. When you spoke to his wife, did you confirm that the credit card information for Terry Muhlenkamp from the database was the credit data of Terry Muhlenkamp?
A. Yes. And just to be clear, this table or a table similar to this table on another command and control server, there were multiple tables like this on every command and control server that we did a search warrant on.
Q. And finally, did you speak with a Larry Kuehl?
A. Yes.
Q. And did you see Larry Kuehl's name on this list?
A. I did, yes.
Q. And when you spoke with Larry Kuehl, did you confirm the credit card information from the database was, in fact, his credit card information?
A. I did.
Q. Now, did you also continue to review other search warrant information that you were receiving?

A. Yes. We issued multiple search warrants for identified command and control servers.
Q. And did you also continue to issue search warrants I think you had said for e-mail accounts?
A. Yes. We did search warrants for e-mail accounts as well.
Q. Did you compare information found in e-mail search warrant returns with the information you were finding on the command and control server search warrant returns?
A. Yes. We compared all the data we had across the case with all the other data we had to see the connections between all of the data.
Q. And how did that analysis help you identify both technical evidence and also identifying evidence?
A. So we could see in the command and control server all the files that were necessary for the botnet to operate, and we were able to see in the e-mail communications that the individuals were talking about files that were on the command and control server.

The e-mails themselves were encrypted, so we were not able to see inside the content, but you could tell by the subject lines that the individuals were using, that they were speaking about either files on the command and control server or credit card data or services they were procuring to support the Bayrob

botnet.

For example, you would have an e-mail from Master Fraud that said "dream BPS," and they were hosting their systems at dream host, so I could tell that that was something to do with dream host.

Q. Okay. Was there ever in search warrant returns for e-mails any unencrypted data that you could review other than subject lines?

A. There was -- I don't believe there was any unencrypted data in the search warrant returns. I believe some of the data provided by AOL had one or two unencrypted attachments, and I believe that's it.

Q. Okay. And how would analyzing those unencrypted attachments be helpful in your investigation?

A. So one of the unencrypted attachments that was sent was what I would refer to as like an accounting spreadsheet that was created by the Bayrob Group to trap their auction fraud and where the money was going and who was getting paid what.

Q. And I would like to show you Exhibit 1741, which has already been admitted. If we could look first at page 1. Looking at the first page of page 1, do you recognize this?

A. Yes.

Q. And could you tell who this e-mail was sent to?
A. This was sent to amightysa@gmail.com.
Q. Who was it from?
A. It was sent from r a 101, p i t p u t i n @ gmail.com.
Q. And were these both e-mails saved under your investigation you associated with members of the Bayrob Group?
MR. O'SHEA: Object.
THE COURT: Sustained.
BY MR. BROWN:
Q. Based on your investigation, did these e-mail addresses have any importance to your investigation.
A. Yes. I knew who the individuals using —
MR. O'SHEA: Objection.
THE COURT: Overruled.
A. I knew who was using these accounts.
Q. Okay. At the time you received this, did you know specific identification?
A. Not at the time that we received this, no. I do now.
Q. Okay. What significance did it have to you at the time you received this?
A. So the e-mail accounts themselves had significance

because they were members of the Bayrob Group.

MR. O'SHEA: Object.

THE COURT: Overruled.

A. The ex-mailer had significance because we had seen that ex-mailer a number of times.

Q. And what's the significance of the ex-mailer, if anything?

A. The tool or the e-mail program used in the generation of this e-mail was Courier with a specific version from Rose City Software, which we had seen previously in the investigation based on information provided by Renotified, for example.

Q. And then did you analyze the contents of the attachment that was attached to this e-mail?

A. I did, yes.

Q. And if you could turn to page 23.

Could you explain what this spreadsheet means to you, the highlighting, the gray part first?

A. Yes. This file is a file called amounts.XLS in the e-mail, and it was an Excel file that was sent between two members of the Bayrob Group that contained information that we had seen before in other places in the investigation, such as the command and control server interviews we had done and based on data related to

financial transactions when wires were sent.

So one of the individuals on this sheet, for example, like Ryan Martin, I had seen that in the database on the command and control servers, and Donna Wolfe was someone we were well aware of in our investigation as a mule for this group, and she was based in Ohio.

MR. GOLDBERG: Objection.

THE COURT: Overruled.

BY MR. BROWN:

Q. What significance did Donna Wolfe have to your investigation?

A. She was one of the intermediaries receiving money from victims and sending it overseas. She would split the transactions up and send those wires overseas?

MR. O'SHEA: Objection.

THE COURT: Sustained at this point.

BY MR. BROWN:

Q. Turning to page 24, what, if any, significance did this page have to your investigation?

A. So again, we saw different transactions, and based on my investigation, I was able to determine that we had victims and the amounts they were paying, who they were paying to, the bank account of the person that was

receiving the money from the victims' address information related to that individual, the dates, and sometimes there was an annotation times 2, and based on my investigation, victim interviews, I interpreted that to be --

MR. GOLDBERG: Objection.

THE COURT: Sustained.

BY MR. BROWN:

Q. Did that review or analysis have any importance to your investigation?

MR. GOLDBERG: Objection.

THE COURT: Yes or no, sir.

THE WITNESS: Yes.

BY MR. BROWN:

Q. What, if any, was that significance?

MR. GOLDBERG: Objection.

THE COURT: Overruled.

A. The significance was that it was different from other lines, and I was aware in certain transactions the Bayrob Group would actually victimize people twice.

MR. O'SHEA: Objection.

THE COURT: Overruled.

A. By -- after tricking them into sending money to an eBay escrow agent, they would respond back and tell that

victim there was a problem with the payment, and that they needed to resend the money.

And eBay would give them a discount of, for example, $500 because of the problem. So instead of defrauding them for $9,000, they would defraud them for $17,5.

Q. And based on your analysis, you saw evidence of that?

A. Based on evidence of the command and control server, e-mails we had seen, victim interviews we did, that's how I assessed that to be.

MR. O'SHEA: Objection.

THE COURT: Overruled.

BY MR. BROWN:

Q. Turning to page 25, was this also — and please zoom out — was this page also part of the e-mail search return?

A. Yes. This was another tab.

Q. And what, if anything, did this have of investigative significance to your case?

A. So this was a sheet that detailed specific members of the Bayrob Group and amounts that they were receiving from this fraud.

MR. O'SHEA: Objection.

THE COURT: Overruled.

BY MR. BROWN:

Q. Based on your analysis, what led you to that conclusion? Withdraw that question.

Is there part of this spreadsheet that was of particular interest to your investigation?

If you could just describe the quadrant, we can bring it up for you?

A. Okay. So for example, the top of the second half —

Q. Okay. Would it be the first —

A. Starting at MF', for example, or a couple lines up here actually.

Q. Eight lines, ten lines down? Is that about good?

A. Sure.

Q. Can you zoom that? And what, if anything, did this mean to you in your investigation?

A. So each of these monikers here were related to individuals, individual members of the Bayrob Group, Master Fraud, Linx or Linxstal —

MR. O'SHEA: Objection.

THE COURT: Overruled.

A. — Min or Minolta 9797 Amy or amightysa, Raul or Rasputin, Natiune.

Q. Okay. And what was the column to the right?

A. This was their percentage.
MR. O'SHEA: Objection.
THE COURT: Sustained.
BY MR. BROWN:
Q. Based on your review and analysis of this record and data you were finding in other e-mails in the command and control server, what, if any, significance did that second column have to your investigation?
MR. O'SHEA: Objection.
THE COURT: Sustained. More foundation.
BY MR. BROWN:
Q. As you were collecting information about the Bayrob Group, did you want to collect evidence about how the money was distributed among the group?
A. Yes.
Q. Was review of this attachment helpful in that part of your investigation?
A. Yes.
Q. How?
A. This data combined with information from other locations in the investigation —
Q. Okay. And — I'm sorry.
A. — and identified the percentages that the individuals in the group were receiving.
MR. GOLDBERG: Objection.

THE COURT: Overruled, but you still need more.

BY MR. BROWN:

Q. And if we zoom out of this, could you tell from where these numbers were being calculated?

Like where the numbers on this spreadsheet were coming from based on your review of the attachment? Just tap, I'm sorry.

A. Based on the document as a whole?

Q. Yes.

A. I could see there was wire transfers on the first half, and I could see what I — based on my analysis was payout numbers on this data.

MR. O'SHEA: Objection.

THE COURT: Side bar. Sorry, folks.

(Side bar held on the record.)

MR. O'SHEA: Foundation. I heard from other sources. That could be 3,000 hearsays.

THE COURT: I still am not clear where that column is coming from, and I agree with Mr. O'Shea, he said in combination with other sources, and I am like — like what sources? I just need — I need more of an explanation.

MR. BROWN: Okay. And there will be two sources. I will have Special Agent Macfarlane, and we

have another witness who can talk about the creation of that data as well.

MR. GOLDBERG: Just for the record, I wanted to say that Nicolescu was also objecting to the foundation.

(Side bar concluded.)

BY MR. BROWN:

Q. Based on your review of page 25, were there any formulas on this page that you recognized?

A. I can't see the page at all.

Q. Sorry.

MR. BROWN: Oh, that's right. There was a side bar. I'm sorry, your Honor. It has been a while since we have been there.

THE COURT: The jury cannot see this, folks. Did you want them to?

MR. BROWN: No, we do. We would like it up.

THE COURT: Oh, okay.

BY MR. BROWN:

Q. Do you recall my question, or would you like me to --

A. There were formulas both within the cells and in the text as well. I mean --

Q. Okay. Based on your review, were there formulas

underlying any of the dollar relay amounts in the table?
A. Yes, but to talk about those, I would have to see the underlying formulas.
Q. Do you know where the numbers used in this formula came from?
A. No. No, I don't know the specific numbers for each cell.
Q. Okay. Now, the column — I think I used the word lei. Did you have an understanding of what a lei is, l-e-i?
A. Yeah. Lei is the Romanian currency.
Q. Okay. And what is Euro?
A. Is the European and Union currency.
Q. Based on those columns identifiers, what do you think those columns contained?
A. That would be money in those currencies.
Q. And do you also see — if we can zoom in on that sort of middle quadrant, do you see columns with USD?
A. Yes. I see columns with USD.
Q. And what do you take USD to mean?
A. U.S. dollars.
Q. Now, at this point in your investigation, what, if anything, were you seeing in the data that was helping

with the identification of members of the Bayrob Group?

A. So at this point in the investigation, I had seen data provided by both AOL, Symantec that identified a mistake that one of the members used when logging into their criminal account and opened 9797.

I had seen references to Minolta and other members of the group that I was aware of in the command and control server, in the data intercept in search warrant data and in data provided by the private sector as well as — no. I think that's it — and PRTTs, pen register trap and traces.

Q. You were seeing e-mails?

A. Yes.

Q. Were you able to link any of those e-mail addresses you were seeing with monikers like the ones you saw in the table here on page 25 of Exhibit 1741?

A. Yes. The Minolta, for example, is a good example of that.

Q. Okay. And what did that linking tell you?

MR. O'SHEA: Objection.

MR. GOLDBERG: Objection.

THE COURT: Overruled.

A. The linking told me that Minolta was, you know, the Minolta 9797 account, which was discussing the same code

on the command and control server, was a member of the group and was using the command and control server.

Q. Okay. And were you able to make any conclusions based on your review of the Master Fraud accounts?

A. Yes. Based on my review of the Master Fraud accounts, it appeared that Master Fraud was directing the show effectively in that he was sending the majority of the e-mails --

MR. GOLDBERG: Objection, your Honor.

THE COURT: Overruled.

A. So based on analysis of all the e-mails, Master Fraud was the top sender. He was sending the most e-mails to other members of the group, and he was involved in almost every e-mail between members of the group.

Q. Based on your review and analysis of the e-mail search warrants, the command and control server search warrants, were you able to determine the activity of any other member of the Bayrob Group or the frequency?

A. Yes. Based on the review of the command and control servers, I was able to also start to understand the roles of what each member was doing.

For example --

MR. O'SHEA: Object.

THE COURT: Overruled.
A. There was a table called "auto listings" that documented which user was responsible for which auction, and you could see that one user was, you know, the primary lister of those auctions.
Q. Do you recall what name was used in that?
MR. O'SHEA: Objection.
THE COURT: Overruled.
A. Min, m-i-n.
Q. And based on your investigation, what did min mean to you, if any?
A. Minolta.
Q. And were you able to determine who or which monikers to which nicknames were more accurate that — were you able to determine if nicknames were more accurate than other e-mails?
A. Yes. So during the entire course of the investigation —
MR. O'SHEA: Object.
THE COURT: Overruled.
A. So I analyzed all the data from the investigation all the e-mail traffic that we had seen, and it was apparent that members of the group came in and out of the group based on that traffic.
So you know, at the beginning, there were a

number of members that were communicating over e-mail about the fraud scheme. When -- approximately at 2013-2014 the group paired down, and only three to four members started talking for the next couple years.

Q. And were you able based on your investigation and review of the data that you received via search warrants, were you able to determine who those three or four members were?

A. Yes. The three primary members that were speaking were Master Fraud --

MR. O'SHEA: Objection.

THE COURT: Overruled.

A. -- amightysa, and Minolta 9797.

Q. And based on your review of the data you received, were you able to identify which nicknames went with which e-mail address?

A. Yes.

Q. For instance --

A. For instance, Master Fraud was MF. Minolta was Min, and amightysa was Amy.

MR. O'SHEA: Objection.

THE COURT: Overruled.

BY MR. BROWN:

Q. Now, based on your investigation of the C and C data, the wiretaps, and the e-mails, were you able to

identify any individuals' identities based on those nicknames and e-mail addresses and connections?

A. No.

Q. Going back to the beginning of your testimony, do you recall testifying about two halves?

A. Yes.

Q. And is the identification sort of the people path you mentioned?

A. Yes. I was hoping that the technical path would lead me to identification, but after reviewing all the connections into the servers, all the data, the data intercept, there was not direct connections back to individuals.

All the connections coming into the command and control servers that I observed were come through multiple layers of proxies.

Q. Did there come a time when you reviewed any investigative materials that helped you identify an actual person?

A. Yes. Concurrently to the technical side of the investigation, I was providing information to the RNP in the form of a legal assistance treaty where we were asking for assistance in identifying individuals related to this group.

Q. Were you talking to any other — or were you

following up on any other investigative leads that your investigation turned up?
A. Yes. We were pursuing the raduspr mistake that occurred and had provided the information that we had gathered, related that specific moniker in one of our requests.
Q. And again, what is the raduspr mistake?
A. So the raduspr mistake was in Minolta 9797 during a log-in session to that e-mail account entered in raduspr and his password, which was the same one for the Minolta 9797 account.
Q. And if I could ask you to take a look at 1742, which I believe is already in evidence, do you recognize — if we could, do you recognize this?
A. Yes, I do.
Q. What do you recognize it to be?
A. It is the session I just described.
Q. Okay. And looking at Exhibit 1742, could you please explain how you knew what you just testified about?
A. So when visiting the site GMX, you have to put in a user name and a password to log in. In this session right here the user name is raduspr, and the password is kill 66 bill.
Q. And based on that information what, if any,

investigative steps did you take next?
A. So I searched internal databases for information related to raduspr. I searched on the internet for information related to raduspr.
Q. Did you serve any legal process?
A. I did. I served legal process to — so from the internet searches, I was able to identify a number of different accounts that was associated with this handle, and we served subpoenas on those accounts.
Q. And specifically who did you serve the subpoenas on?
A. Served subpoenas on Twitter, Facebook, and Yahoo.
Q. And I would like to — did you receive any information in return from those subpoenas?
A. Yes.
Q. And I would like to have you look at, before we publish to the jury, 1755. Do you recognize this?
A. I do.
Q. What do you recognize it to be?
A. This is the return from the Yahoo subpoena for the user raduspr.
Q. Did you create any of this information?
A. I did not, no.
Q. Is this a fair and accurate copy of the Yahoo return

information you received?
A. It is, yes.
MR. BROWN: Permission to publish this to the jury, your Honor?
MR. GOLDBERG: No objection.
MR. O'SHEA: Objection.
THE COURT: You are objecting?
MR. O'SHEA: I am, your Honor.
THE COURT: Objection overruled. I will allow it.
BY MR. BROWN:
Q. And could you explain what information you received back from Yahoo?
A. So this data is from a subpoena return from Yahoo for the log in raduspr. It had the associated account that was subpoenaed. It had a backup for a secondary account on that, on the raduspr@Yahoo.com account, verified means that Yahoo had actually sent a confirmation link out to that gmail account?
And that gmail account clicked the link to confirm that both raduspr@Yahoo.com and raduspr at gmail.com were controlled by the same person or had access to the same account.
Q. And what was the importance of verifying the accounts?

A. The importance of a verified account is that it is an alternate communication mechanism for this account, and if you were able to — say for example, you lost your password to this account, they could send you a like password reset to an alternate account.
Q. What other information were you able to learn from this subpoena return?
A. So there was a phone number associated with it and address and a name.
Q. And what was the significance of the phone number, if anything, to your investigation?
A. At the time of receiving this subpoena, it was not information that we had seen other places, but by the end of the investigation, we associated that phone number with Radu Miclaus.
Q. Okay. Now, you said you also did an open search investigation?
A. Yeah. I searched the internet for this handle, raduspr.
Q. Okay. And among other things, open search, is the technical term Googling?
A. Yes. I Googled raduspr.
Q. And what, if anything, did you find from your open source research?
A. So I was able to confirm a number of the pages that

were provided by both Symantec and AOL so the Twitter account and the forum that was related to motor vehicles.

Q. Okay. I would like to show you what has been, I believe, admitted as 1448.

THE COURT: 1448?

MR. BROWN: Yes, ma'am.

Q. Do you recognize that?

A. Yes.

Q. What do you recognize this to be.

A. So this was the Twitter account for raduspr.

Q. And what about this was important to your investigation?

A. There were a number of things important. The user name obviously, the profile pick was important, the name. It is important to understand when that individual joined, how many people were following that individual, and specifically the posts.

Q. And what about this post was relevant to your investigation?

A. Well, the profile pick, we were able to later link to a profile pic or a picture we found on Radu's phone, Radu Miclaus' phone, and Ypool was referenced in multiple places on the command and control server as well as in the e-mail.

Q. Based on your investigation, what did you understand Ypool to be?

MR. O'SHEA: Objection.

THE COURT: Overruled.

A. So Ypool was a cryptocurrency pool, and a cryptocurrency pool is — I think it was described earlier as being similar to a lottery pool where individuals that are mining cryptocurrency can join a group, and they can share — as being part of that group allows them to share in splitting the proceeds from the activity they were involved in.

So if, for example, there was a pool of a hundred people and I had ten systems that I joined to the group and the pool of 100 made a thousand dollars, I would ten percent of that one thousand dollars.

It was just really a way to split the proceeds, to have better chances of actually getting paid and then splitting those proceeds, increasing your odds at that point.

Q. Is it fair to say the more power you provide, the bigger your share?

MR. GOLDBERG: Objection.

THE COURT: Sustained.

BY MR. BROWN:

Q. What, if anything, did you do based on this — the

information software?
A. So based on the information, I issued a subpoena to Twitter as well.
Q. And did you get information back from that subpoena?
A. I did, yes.
Q. Without publishing to the jury, what we see is Government's Exhibit 1750. Do you recognize that?
A. Yes. That's the subpoena return.
Q. What do you recognize that to be or return from?
A. This is from Twitter.
Q. And how do you know the subpoena return is from Twitter?
A. The format of it.
Q. And did you add any information to this?
A. No.
Q. Did you modify any information?
A. I did not, no.
Q. Is this a fair and accurate depiction of the subpoena return you received from Twitter?
A. Yes.
MR. BROWN: Permission to publish to the jury, Judge?
MR. O'SHEA: A moment, Judge.

THE COURT: Certainly.

MR. BROWN: It would just be page 1, your Honor.

MR. O'SHEA: As to page 1, just page 1, no objection.

THE COURT: Mr. Goldberg?

MR. GOLDBERG: No objection.

BY MR. BROWN:

Q. Special Agent Macfarlane, taking a look at page 1 of 1750, what, if anything, was of importance to your investigation?

A. So the e-mail account was the important aspect of this. It just confirmed that this user also was the user of the raduspr@Yahoo.com account.

Q. Was there importance to you in the time zone of Bagdad? Did you do any further research on that?

A. I am sure I did, and unfortunately, I don't have those notes with me.

Q. Did you learn if any other cities were in the time zone of Bagdad?

A. Yes. It is the time zone that a portion of Romania is in as well.

Q. Now, did your open source research provide you with any other relevant data? Withdraw that.

Did your open source research provide you

with any other information of interest to your investigation?
A. I believe I found like a Free Lancer page as well.
Q. And what, based on your investigation, is Free Lancer?
A. Free Lancer is a place where you can advertise a skill set and advertise yourself to be hired for jobs as a free lancer.
Q. Is it a criminal page?
A. No. It is not criminal.
Q. It is a job listing. Instead of a want ad, it is like —
A. Like an online resume.
Q. Without publishing to the jury, can you review, look at Exhibit 1747?

THE COURT: I'm sorry. One more time.
MR. BROWN: 1747, your Honor.
THE COURT: Thank you.
MR. BROWN: Thank you.

BY MR. BROWN:
Q. Do you recognize this?
A. Yes.
Q. How do you recognize this?
A. This is the page.

Q. Did you create any of this data?
A. No.
Q. Is this page the same page that you had on the internet?
A. Yes.
Q. Is it a fair and accurate representation of the web page?
A. It is.

MR. BROWN: Permission to publish?
MR. GOLDBERG: Objection.
MR. O'SHEA: Objection.
THE COURT: Give me one word.
MR. GOLDBERG: Foundation with this exhibit.
THE COURT: Foundation with this exhibit.
MR. GOLDBERG: Sorry.
THE COURT: Overruled. I will allow it.

BY MR. BROWN:
Q. And could you first zoom in on the middle section? And what, if any, information in this zoomed in section was of interest to your investigation?
A. So the profile name, the country.
Q. Okay.
A. The —
Q. I'm sorry.
A. A number of these fields to include some of the

information related to the Python developer aspect.
Q. Based on your training and experience, what did Python developer mean to you?
MR. O'SHEA: Object.
THE COURT: Sustained.
THE WITNESS: This person — oh, I'm sorry.
BY MR. BROWN:
Q. Special Agent Macfarlane, in your experience as an FBI agent, prior to joining the FBI, did you have any knowledge of the term Python?
A. Yes.
Q. Based on that training and experience, did the Python developer mean anything to you based on that experience?
A. Yes. This profile detailed someone who could develop.
Q. Based on the entirety of this e-mail page and your knowledge, training, and experience in the field of computers and computer programming, was Python developer used in a manner consistent with somebody looking to be hired to use computer skills?
MR. GOLDBERG: Objection.
THE COURT: Sustained.
BY MR. BROWN:
Q. Based on your training and experience, was the use

of Python developer consistent with the job raduspr was looking for?

MR. GOLDBERG: Objection.

THE COURT: Sustained.

BY MR. BROWN:

Q. Can we zoom out and look at the bottom half skill down below?

What, if any, information contained in this field was of interest to your investigation?

A. So the specific skills that caught my eye when I viewed this page were PHP, Java, JavaScript, JSP, website design, website security.

Q. And what about those terms were of interest to your investigation?

A. Because those skills were directly relevant to the way in which the Bayrob botnet was developed.

Q. Now, based on that, what, if any, investigative steps did you take to continue to identify members of the Bayrob Group?

A. So based on this information and the location data that was contained within these pages --

MR. O'SHEA: Objection.

THE COURT: Overruled.

A. -- we sent a request for assistance to the Romanian National Police.

Q. And based on that request, what, if any, steps did you take next?
A. Based on the request and the related response, we ran checks on three individuals internally.
Q. And which three individuals did you run checks on internally?
A. An individual by the name of Radu Bogdan Miclaus, Tiberiu Danet, and Bogdan Nicolescu.
Q. Now, based on your research, your open source research and subpoena research, did you at this point in the investigation have an idea of who Minolta was?
A. Yes.
Q. And what was that based on?
MR. O'SHEA: Objection.
THE COURT: Overruled.
A. That was based on traffic provided by AOL. It was based on the related websites that were identified using the raduspr handle, the underlying subpoena returns related to that as well as information provided by the Romanian National Police as a result of the M-LAT process.
Q. Based on that information, what names and nicknames did you associate with Minolta 9797?
MR. O'SHEA: Objection.
THE COURT: Overruled.

A. Radu Miclaus.
Q. Any other names that you saw as a result of your investigation?
A. Raduspr, Min, Minolta 9797, I think that's it.
Q. Based on your investigation, you had testified, you believe, there were three or four members?
A. That is correct, yes.
Q. Who were the remain — was Minolta 9797 one of the four members based on your investigation?
A. Yes.
Q. Who were the other two core members at this point in your investigation?
A. The other two core members were amightysa and Master Fraud.
Q. Okay. And what other nicknames at this point did your investigation associate with amightysa?
A. Amy.
Q. And any others?
A. I don't think — not that I can think of at this time.
Q. And at what point or at this time in your investigation, what other nicknames did you associate with Master Fraud?
A. MF.
Q. Any others?

A. At this time, no.
Q. Were you able to link any of those nicknames to the other individuals the Romanian National Police gave you, the names the Romanian National Police gave you.
A. Initially, no.
Q. Okay. What, if any, investigative steps did you take to make connections?
A. So based on the information that we — the next steps that we took were to search the individuals that were provided, and we determined that Tiberiu Danet had actually been to the United States as an intern for Google.
Q. And what, if any, importance did that give you to this investigation?
A. It told me that he traveled, so I knew that that individual traveled, and that was important to our investigation. Whenever subjects travel outside — into the U.S., that's an investigative opportunity.
Q. And based on that knowledge, what, if anything, did you do?
A. So we set up alerts with the customs and border patrol on the individuals so that we could see if they were traveling into the U.S.
Q. Okay. And based on those steps, what, if any, results did they have?

A. So we were alerted that Tiberiu Danet was traveling into the U.S. through Miami in May of 2015, I believe.
Q. And based on that knowledge, what, if any, steps did you take?
A. So knowing that he was coming into the country, we obtained a search warrant for his effects during the border crossing.
Q. Were there any other investigative steps you took related to this information?
A. Not that I recall at this time.
Q. When you say you got a search warrant for his effects, was that search warrant executed?
A. Yes, it was at Miami International Airport.
Q. And when was it executed at the airport?
A. We executed that search warrant when he came through secondary at the airport.
Q. How did you confirm when he was coming through secondary?
A. Because he had presented travel documents when he was coming through.
Q. Did you conduct surveillance within the airport?
A. We also conducted surveillance on him, yes.
Q. And I would like to show you, without publishing to the jury, Government's Exhibit 382.

MR. O'SHEA: What was that again?

MR. BROWN: 382. I'm sorry. 385. I will come back to 382.

THE COURT: So —

MR. BROWN: 385, your Honor, which has been admitted.

BY MR. BROWN:

Q. Do you recognize this picture?

A. I do, yes.

Q. And what do you recognize it to be?

A. This is a picture of Tiberiu Danet.

Q. And using the little cursor, can you point to Tiberiu Danet?

A. That guy right there. (Indicating.)

Q. Can you describe him a little bit?

A. Sure. He is wearing black shoes, lighter jeans, a white T-shirt with black markings carrying a black backpack, dark hair; really can't tell the height based on this picture.

Q. And you said you had — you executed the search warrant after customs, after he went through customs?

A. Yes, prior to the customs process.

Q. Can you explain what happened during the execution of the search warrant?

A. Yes. So Tiberiu Danet was pulled into secondary screening, and his personal effects were obtained from him, and we searched those effects. We searched the phone, took an image of the phone and other personal items to include a key, a specific key that he carried with him as well.
Q. So you searched the effects?
A. Yeah, we searched his effects.
Q. And you searched a phone?
A. Yes. We took an image of the phone and searched the phone.
Q. Can I show you Exhibit 382 and not publish to the jury?
MR. BROWN: 382, is that admitted, your Honor?
THE COURT: Yes.
BY MR. BROWN:
Q. Could you pull up Exhibit 382? Do you recognize this?
A. Yes. This is Tiberiu Danet's phone.
Q. And how do you recognize it to be Tiberiu Danet's phone?
A. I was the one that put the tape on it.
Q. Why did you put the tape on it?
A. Just in case the phone set up to record or listen.

I put the tape on it just in case the video camera or the microphone was set up to record or listen.
Q. Do you do that every time?
A. In certain circumstances, yes.
Q. What are those certain circumstances?
A. When we are dealing with highly technical individuals.
Q. Now, did you, in fact, search the — when you say you searched the phone, what do you mean by that?
A. We took an image of the phone and had specialized personnel from Miami come and create a digital image of the phone, and they imaged the phone itself as well as any removable media within it.
Q. And did that imaging capture all the data on the phone?
A. Yes.
Q. Everything?
A. To my knowledge, yes.
Q. And did you then search that image?
A. Yes.
Q. And what, if anything, of relevance for this investigation did you find on Danet's Miami phone?
A. So contained on this phone was instant messaging, and based on all the investigation that I had done so far, it is the first time I was able to see two members

of the Bayrob Group talking to each other about code on the command and control server in an unencrypted format.

Q. How were you able to see that?

A. So as part of the imaging process, the files on the phone are pulled off and made into a forensic image, and those files contained that data. So I was able to use a tool to view the data that were in those files.

Q. Okay. Now, what applications were they using?

A. So the phone had a number of applications on it, but the one that was important to the investigation was a tool called Xabber which is spelled X-a-b-b-e-r.

Q. And what is Xabber?

A. So Xabber is an instant messaging tool that allows two or more individuals to instant message with each other over the Jabber protocol.

So the Jabber protocol is like the language it speaks, and the application itself is called Xabber, X-a-b-b-e-r.

Q. So a Xabber chat happens to be in a Jabber application?

A. Exactly.

Q. And is Xabber typically encrypted?

A. Xabber can be encrypted, so it has the ability to support off the record or OTR chats.

Q. And can Xabber be spelled any other way?
A. Not that I am aware of.
Q. And were you able, in fact, to review Xabber chats?
A. I was, yes.
Q. And based on the review of Xabber chats, were you able to observe information relevant to this investigation?
A. Yes.
Q. Were those Xabber chats encrypted?
A. No. No, they were not.
Q. And how did you know the messages you reviewed were related to the Bayrob Group?
A. I knew the messages were related to the Bayrob Group because the chats were discussing specific extremely unique files that were found on the command and control servers.
Q. Now, I would like to show you without publishing to the jury page 714 of Exhibit 367. And first, could we zoom in on —
MR. BROWN: Can I use the Elmo, your Honor?
THE COURT: Sure.
MR. BROWN: And this will not be published to the jury, right?
THE COURT: Right.

MR. BROWN: Sorry, your Honor. You are missing out on my excellent Elmo — but we have it.

BY MR. BROWN:

Q. Do you recognize this?

A. Yes.

Q. How do you recognize this?

A. So this is data that is coming directly out of the database.

Q. Of what?

A. Of the Xabber application.

Q. And is the Xabber application on the seized telephone?

A. Yes.

Q. And was this data produced by you?

A. No.

Q. Was this data modified my you?

A. No.

Q. Was this data formatted my you?

A. No.

Q. Is this a fair and accurate representation of the data that was imaged from the Danet-Miami phone?

A. Yes, with one exception.

Q. Yes.

A. That this — the fourth column of this exhibit

contains a translation that was not present in the original.

Q. So you added a column?

A. A translator did, yes.

Q. And how was that column added to that data?

A. So this data was provided to our translation services, and our translation services translated this data for us.

MR. BROWN: Your Honor, permission to publish to the jury?

MR. GOLDBERG: No objection.

MR. O'SHEA: No objection.

MR. BROWN: Thank you.

BY MR. BROWN:

Q. Okay. And so looking at the far left column, what is that based on your investigation and review of the search warrant material?

A. So based on a review of the phone, I was able to identify the accounts that were on that phone related to different services, and one of those accounts was an account romeo-mobile @ ro.remote.mx.

Q. And were you able to determine, based on your review of that data, who the owner of that account was?

A. Yes. That was an account of Tiberiu Danet. It was on his phone, and that was the account for that Xabber

client.
Q. And looking at — the next column over, column 2, what was — what is that information?
A. Column 2 is who this person was chatting with.
Q. And just looking at that column, who is he chatting with?
A. He is chatting with obe.m@ro.remote.mn.
Q. Okay. And were you able to, based on your review of the data in the cellphone, determine who the users of obe.m was?
A. Based on my review of the cellphones, no, I don't believe I was
Q. Now, looking at the far right column, what, if anything, was of relevance to your investigation?
A. So the conversation between these two individuals was of relevance. Specifically what brought my attention was when they were talking about a protocol and not having to modify the server.
Q. And how, if in any way, was that relevant to your investigation at this point?
A. Because we had identified these individuals as associates of Bogdan Miclaus, Radu Bogdan Miclaus, and we knew at that point in time that Radu was Minolta 9797.
MR. O'SHEA: Objection.

THE COURT: Overruled.

A. And these — this was one of his associates that had been provided by the Romanian National Police. This individual was very technical based on the review and his internship at Google, and this conversation to me started to confirm some of that information related to indicating he may be part of this group.

Q. Now, looking at page 175 —

THE COURT: You know what, at this point, I think we are going to take our morning recess.

Please remember the admonition. All rise for the jury.

(Recess had.)

THE COURT: Please be seated. Folks, I apologize for that being a little longer than normal. I ended up on a telephone call that I just couldn't end, so I apologize. It was my fault, nobody else's. You can continue.

MR. BROWN: Thank you.

BY MR. BROWN:

Q. If you can look at page, 715 line 26515, was there anything of interest in your investigation?

A. So starting at 26515, we see — well, what do you want to do" and then following up, the response is "to spawn it and again" and then, they are talking about —

MR. GOLDBERG: Objection.

BY MR. BROWN:

Q. Was there anything of the three or four lines of chat relevant to your investigation?

A. Yes. Based on my 15 years of experience and analyzing code related to cyber crime as well as to code in general, I was seeing programming terms and something that I see often related to the running code on systems.

Q. And what phrase or word was that?

A. "Create process."

Q. Now, turning to page 716, did you review these chats?

A. I did, yes.

Q. Were there chats on page 716 relevant to your investigation?

A. Yes, they were.

Q. And which lines were those?

A. The most important one on this page is 26530.

Q. And what is that?

A. A miner force.

Q. And why was that important?

A. This term was all over the control server. At this point in our investigation, the Bayrob Group was evolving, so starting at the end of or in approximately

2013, the Bayrob Group was no longer actively engaging in the auction fraud.

In 2014 and 2015, they had changed direction. My reviews of the search warrants, each search warrant that I would do on the command and control server showed a new evolution into additional functionality.

And one of those components was cryptomining. So one of the ways in which the Bayrob Group botnet was making money was via using infected systems to mine cryptocurrency on the command and control servers that I was seizing around this time, and I was seeing that specific term within the database, in cod, and a it was related to the running of cryptocurrency miners on infected systems.

Q. Okay. And if he could pull up and publish to the jury 1886, 1-8-8-6, do you recognize that?

A. I do, yes.

Q. How do you recognize it?

A. This is a screenshot of me analyzing one of the databases on one of the command and control servers.

Q. And did you create this data?

A. No. The data was there when I arrived.

Q. Did you modify this data?

A. No.
Q. Did you format this data in any way?
A. I pulled specific columns from this table, but I didn't change the data in any way. I am just showing a subset of the data.
Q. Did you do this by hand, or did you use a program to create this?
A. So the — this statement right here is what I am selecting out of that table. So I am selecting columns, if you can think of this like a spreadsheet almost, I am selecting the column SOCKS ID and miner force time from the database obtained from that system and that table, which is the SOCKS 3 underscore ping table where this condition is met, which a miner force time, miner underscore force time.
Q. In making that request, did you modify or change the data?
A. I did not, no.
Q. Does Exhibit 1886 display the data as it existed on the command and control server?
A. Yes.
Q. Is it a fair and accurate representation of the data that occurred on the command and control center?
MR. GOLDBERG: Object.
THE COURT: Overruled.

A. Yes.
Q. Did the format you put it in help you in your analysis?
A. It did, yes.
Q. Did it change the data at all.
A. It did not.

MR. BROWN: Permission to publish 1886 to the jury?

MR. GOLDBERG: No objection.

MR. O'SHEA: No objection.

BY MR. BROWN:

Q. Special Agent Macfarlane, could you describe what Exhibit 1886 is?
A. Yes. This is a view that I — I took this screenshot when I was analyzing the database on the command and control server. This section over here are the associated tables that were found on the command and control server.

This is a statement that I issued against the SOCKS three ping table, which contained information on the infected systems, and I pulled just a couple of columns from that table to view.
Q. So what is the SOCKS ID column?
A. Based on my view of the infrastructure, it is a unique ID given to each individual infected

system.
Q. So that's an infected computer?
A. Yes.
Q. Okay. And what is the miner force time?
A. That's a numerical representation of when the functionality of that botnet was run, so you can think of it in layman's terms, on this system, this was the time that miner was instructed to run.
Q. So looking at that what were you able to tell that was useful to your investigation?
A. Primarily at this point in the investigation miner force was unique and important to the operation of the botnet.
Q. Did you make any conclusions based on your investigation at this point what those individual infected computers were doing based on this page?
A. Yes. These systems were instructed to mine cryptocurrency.
Q. So they were mining at this time.
A. Yes. They were instructed, they were given the command to mine cryptocurrency.
Q. Now, if we can go back to Exhibit 367, page 716, were there any chats — and this is back to the Xabber chat —

A. Yes.
Q. — and looking at page 716, were there any chats that were of interest to your investigation? I meant page 717, I apologize. —
A. Yes. I'm sorry. On 717, the context is it matters. So the conversation almost on this entire page is important, but the key element would be this file extension down here so line 26560 when you do that .exe.dep.
Q. And what did that mean in your investigation?
A. This was a specific element that I had seen on other locations on the command and control server.
Q. Based on your investigation, what did you see the .exe.dep in this relationship to Bayrob and Trojan?
MR. GOLDBERG: Objection.
THE COURT: Overruled. Was there an objection?
MR. GOLDBERG: Yes.
THE COURT: I thought so.
A. So .exe.dep was a file extension that I found referenced within the command and control server in numerous places, specifically related to what I viewed as plug-ins or modular functionalities, modules for the virus.
So my analysis of how the entire — the

virus interacted with the command and control server showed that the virus could download additional functionality.

It could be commanded to say, "hey, infected system, you need to download this plug-in and run it, and this .exe.dep was directly related to files associated with that activity.

Q. How was it directly related?

A. It was the file extension of some of those files.

Q. Do you recall the testimony — do you recall hearing testimony about — about file extensions?

A. Yes.

Q. What's the purpose of a file extension?

MR. GOLDBERG: Objection.

THE COURT: Overruled.

A. A file extension helps an operating system figure out what application it needs to run.

Q. And what was the importance of seeing .exe.dep in a file extension in this chat?

A. The uniqueness of this specific string was unique because the .dep file extension, I had never come across it. I had never seen it anywhere. I researched it. There is no application that uses it.

It is not — if you Google .exe.dep, you are not going to find anything legitimate that uses it. As

far as I could tell, it was like unique to this specific group.

Q. Now, showing you 2069 without publishing to the jury, do you recognize that?

A. Yes.

Q. How do you recognize it?

A. This is code that I found on the command and control server, one of many files containing code that supported the Bayrob product.

Q. And how do you recognize it to be Bayrob code?

A. I recognize it because I analyzed thousands of files on these command and control servers?

And I can tell by the specific commands that they directly relate to the operation of the botnet.

Q. Did you create any of the data or any of the code in this exhibit?

A. I did not.

Q. Did you modify any of the data or any of the code in this exhibit?

A. No.

Q. Did you format any of the data or code in this exhibit?

A. The viewer that I used to view this may have like wrap lines, for example, but no, I didn't specifically

change the format in any way.

The text viewer that I used to view it would -- it has to wrap lines -- some of these lines may be real long, and it would wrap those lines, so from a formatting standpoint, that could occur.

Q. Was the formatting for analysis purposes just so it would fit on a page?

A. Yes. Just so like you could see it.

Q. Did it format or change any of the data?

A. It did not.

MR. BROWN: At this point, I would like to publish 2069.

MR. GOLDBERG: No objection.

MR. O'SHEA: No objection.

BY MR. BROWN:

Q. And Special Agent Macfarlane, what is 2069?

A. So this is code that was related to interacting with infected systems. So it would be responsible for helping infected systems do what the Bayrob Group wanted them to do effectively.

I mean, this is the controller effectively, one of the files that was controlling the infected system.

Q. So this is how orders would be pushed out?

A. Yes. And there were a number of files that sort of

supported this file, but yes, this was one of the main files that was responsible for like the infrastructure.
Q. Okay. Now, looking at the top of the page, what, if any, significance to your investigation was that sort of carat, question mark, .PHP?
A. So this was the language that the code was written in.
Q. Is that .PHP language?
A. Yes. So .PHP is a web scripting language, so with .PHP, what happens is that if you have a .PHP file and you view it in a web browser, it provides the capability of having a more — if I can — a dynamic web page or a web page that can do additional things.
Q. Okay. And if we look down, about halfway down the page, do you see the words "function ping"?
A. I do.
Q. And what, if any, importance does the function ping have?
A. So this function is a function that — so I will step back.

A function is like a smaller block of code that runs like a specific task, if you will.
Q. Was this casting a ping to do a ping?
A. It was just the naming convention that the Bayrob Group used for this, but yes, usually what the functions

are named after, they're what they do.
Q. Okay. And as you have seen in Exhibit 1137, a ping is when the command and control server would reach out to an infected computer?
A. Yes. A ping effectively in layman's terms is, you know, "check in, are you there?"
Q. Okay. And what are the lists of — is it six, eight things starting with global — what importance was that?
A. So these are variables that, based on the value of those variables, the infected system that checked in would do different things.

For example, based on the miner force variable, the system would do something related to cryptocurrency mining.
Q. And that's based on — withdraw that.

Now, in this exhibit, did you see any evidence of the .exe.dep extension?
A. Yes. It was in here.
Q. And do you know the importance of it being present in this exhibit?
A. Yes. It was related to some of the plug-ins. So there is a statement in this code that allows an infected system, based on parameters set for that infected system, to receive a plug-in based on configuration.

So it is important to note that this file would also interact with the database. So data in the database would sort of determine how this page instructed the infected systems to do various functions.

Q. So the .exe.dep was used in this code based on your review to issue commands and direct commands to be issued?

MR. GOLDBERG: Objection.

MR. O'SHEA: Objection.

THE COURT: Sustained.

BY MR. BROWN:

Q. How would you describe the role of the .exe.dep file in this code?

A. So in this code, there is a section that references files on the command and control server, and if the condition is met, the infected system would download the related file that ended in .exe.dep.

Q. Okay.

A. And I believe, if my memory serves me correct, it is at the end of this file.

Q. Okay. And in fact, if you turn to page 17, do you see -- if you could blow up the page -- do you see files with .exe.dep?

A. Yes.

Q. And what sort of files are -- have that file

extension?
A. So we see at the top of this page, we see miner force .exe.dep.
Q. What would the .exe.dep do for miner force?
A. In this case, it is a naming convention, so this extension is just a way they named this file. The extension would help this code figure out, you know, what plug-in to pull at this location.
So it would go into the command and control server and from the plug-ins directory pull the miner underscore force .exe.dep.
Q. Is that the same role that .exe.dep would serve for win defender lower in the page?
A. Yes. So essentially, this shows the naming convention of all the different plug-ins in the plug-in directory. This is how they name some of their plug-ins.
Q. And you testified that this naming convention was unique based on your research and your investigation to the Bayrob Group and the Bayrob Group Trojan?
MR. O'SHEA: Objection.
THE COURT: Sustained.
BY MR. BROWN:
Q. Was this naming convention based on your investigation unique to the Bayrob Group?

MR. O'SHEA: Objection.
THE COURT: Sustained.
BY MR. BROWN:
Q. What did your investigation show about this extension naming?
A. My investigation showed that this extension was like a fingerprint essentially —
MR. O'SHEA: Objection.
A. — for the Bayrob Group.
THE COURT: Overruled.
BY MR. BROWN:
Q. Based on your investigation and your training and experience in the FBI and beforehand, why is it important — what is the importance, if any, of a unique naming convention?
A. It shows a direct connection between the conversation that was happening over chat and the files on the command and control server.
Q. Now, going back to 367, page 722 —
MR. BROWN: Before we publish, can we make sure we redacted everything, your Honor?
MR. O'SHEA: What exhibit again?
MR. BROWN: 367. Before we publish —
THE COURT: You don't want it on?
MR. BROWN: No. We want to make sure we

redact properly, and then we will publish it.

And at this time, I would like to publish this to the jury.

THE COURT: Mr. Goldberg?

MR. GOLDBERG: No objection.

MR. O'SHEA: No objection.

BY MR. BROWN:

Q. Special Agent Macfarlane, do you recognize these chats from Exhibit 367?

A. I do, yes.

Q. Were there any lines of interest for use to your investigation in these chat rooms?

A. Yes.

Q. Now, which lines were of use to your investigation?

A. So these first two lines where the romeo-mobile and obe.m are talking about sequel is relevant because the database was a sequel database and, more importantly, when they are talking about epoll.

Q. And again, who is this chat between?

A. This chat is between Danet and Tiberiu Danet and obe.m@ro.remote.mx.

Q. Based on your investigation of these chats, was your investigation starting to develop a picture of the role of Danet in the investigation?

A. Yes. He was a member of the group that was talking

at a technical level. So he was involved in the technical operations of the Bayrob botnet.

Q. Okay. And likewise, based on your investigation, were you starting to develop an investigative picture of the role of obe.m?

A. I was.

Q. And what was that?

A. So obe.m was a technical member of the Bayrob Group botnet, and some of these chats obe corrected Romeo, which I thought was interesting.

Q. Why was that of interest?

A. Because then Danet was really smart, and I was — knowing Danet and his background and of his internship at Google — and we had also identified his role in the informatics Olympiad at this point — I was just surprised that somebody was essentially smarter than him.

Q. What is epoll? Why was that of interest?

A. Epoll was another file I found on the command and control server.

Q. Okay. And based on your view of the command and control server, what did you — why was epoll of interest?

A. Epoll was of interest because it played an important role related to the use of the infected systems as

proxies.
Q. In layman's terms, what does that mean, Special Agent Macfarlane?
A. So it was a tool that was supporting the Bayrob's botnet ability to relay traffic through infected systems.
Q. Now —
MR. BROWN: One moment, please.
(Pause.)
BY MR. BROWN:
Q. Based on your prior review of e-mail search warrants, were any of the subjects that you saw in the chats of interest to the search warrant e-mail data you reviewed?
A. Yes. There were references to epoll and other chats contained within this phone that also were being talked about over the criminal e-mail accounts.
So we would see subject lines that contained epoll for something, a subject containing epoll.
Q. For instance, could you look at, before we publish, look at Exhibit 1854?
MR. BROWN: Your Honor, could you turn on the Elmo?
BY MR. BROWN:
Q. Did you review search warrant data obtained from GMX

on e-mails belonging to a Master Fraud account?
A. Yes.
Q. And did you review that data?
A. I did.
Q. Looking at page 93 of Exhibit 1854, do you recognize that?
A. I do.
Q. What do you recognize it to be?
A. So this is a log of e-mails between members of the Bayrob Group.
Q. Did you create the e-mails within this log?
A. No.
Q. Did you alter the data in this log?
A. No.
Q. Did you format the data in this log?
A. Yes for reviewing.
Q. And did the formatting change any of the data?
A. It did not.
Q. Did it ease in the review and analysis?
A. It did.
Q. And is this data a fair and accurate representation of the data used from the search warrant return?
A. Yes.
MR. BROWN: At this time, I would like to publish Exhibit 1854.

MR. GOLDBERG: No objection.
THE COURT: Just this page?
MR. BROWN: Yes, your Honor.
THE COURT: 93?
MR. BROWN: Page 93.
THE COURT: Mr. Goldberg?
MR. GOLDBERG: No objection.
MR. O'SHEA: No objection.

BY MR. BROWN:

Q. Looking at July 23, 2015, did you see any e-mail traffic of interest to your investigation?

A. Yes. So the e-mail traffic that was provided through the search warrants was like one half of a puzzle.

So you had data on one side related to the communications about what was going on in the command and control server.

So they were talking about things that I was seeing on the command and control server. Specifically -- and what the command and control server was doing. So at this time, based on our investigation, we had seen that the command and control server was mining various cryptocurrencies?

And on this line, we see BTC addresses. BTC stands for bitcoins. It is the common short name for

bitcoin and associated encrypted attachments. On the following line, I see reference to epoll, which was discussed over chat.

Q. And did the "to" and "from" lines tell you anything useful to your investigation?

A. Yeah. The "to" and "from" line beyond just who sent it and who received it helped me understand the roles of each individual within the group.

Q. And based on your investigation, what roles did you understand amightysa to have?

A. So amightysa was involved in development and was working on some of the .PHP code, was working on some of the content that would get pushed to infected systems, the plug-ins and other technical tasks of versions related to the botnet.

Q. Okay. Now, at this time after Danet came to Miami, what investigative steps, if any, did you take next to further identify the monikers, the remaining monikers you know, the amightysa, the Master Fraud with Danet or Nicolescu?

A. So around this time, based on the chat messages that we saw in the phone blogging into Tiberiu Danet, it was my assessment that he was one of the remaining two members of the Bayrob botnet that was currently active during this time?

And during this time, it was amightysa, Minolta, so in this exhibit, Minolta 2 here is actually using John Doe at tech center instead of Minolta 9797.

Q. Okay. So these conversations were between the three monikers you had identified?

A. Yes.

Q. And at least two people you could connect to?

A. The core group.

Q. And the third person?

A. Was obe, and I didn't know exactly who obe was.

Q. At this point, what steps were taken in the investigation?

A. Based on requests to the Romanian National Police, we received information back that identified that Bogdan Nicolescu --

MR. GOLDBERG: Objection.

THE COURT: Sustained.

BY MR. BROWN:

Q. Did you further transmit information to the Romanian National Police?

A. Yes.

Q. Based on those responses, what investigative steps did you take next, if any?

A. So based on that response, I was able to associate

the handle obe to Bogdan Nicolescu.

MR. GOLDBERG: Objection.

THE COURT: Overruled.

BY MR. BROWN:

Q. How did you make that connection?

A. I made the connection based on the data that was provided to me through the supplemental request.

Q. And based on that information, what steps, if any, did you take next?

A. So having identified both sides of this conversation, I still didn't know who was who. So out of this group, I didn't know whether Tiberiu Danet was amightysa. I didn't know if he was Master Fraud, and I was trying to figure out essentially who was who.

Q. At this point in your investigation, based on all of the information you had received from the search warrant to the Title IIIs and the data from other agencies for organizations, were you confident that you had identified the three-four individuals of the Bayrob Group?

MR. GOLDBERG: Objection.

MR. O'SHEA: Objection.

THE COURT: Overruled.

A. So --

THE COURT: Yes or no, sir.

THE WITNESS: Yes.
BY MR. BROWN:
Q. And again, based on your review of the data you had reviewed from the search warrant returns, Title III, and data from the investigation, were you able to identify the monikers used by the members of the Bayrob Group, the core members of the Bayrob Group?
A. Yes. I knew who the active members of the Bayrob Group were at this point in time in the evolution of the Bayrob Group.
Q. Based on those identifications, was any action taken?
A. Yes. We indicted the following or these individuals as members of the Bayrob Group.
Q. And were they arrested if you know?
A. Yes. They were arrested at the -- based on a request to the Romanian National Police.
Q. And pursuant to their arrests, were searches done of items from their houses or on their persons?
A. Yes.
Q. I would like you to look at Exhibit -- pursuant to an arrest of Tiberiu Danet, do you know if any hard drives were received from him?
A. Can I check my notes?
Q. Yes.

A. Yes, there were hard drives seized.
Q. Do you recall if a Western digital Passport hard drive was recovered from Tiberiu Danet?
A. Yes.
Q. Do you know if the hard drives recovered and the devices recovered were imaged?
A. Yes.
Q. Did you review the images of the devices received from all three members?
A. I did.
Q. Do you recall reviewing data recovered from a Western digital Passport hard drive owned by Tiberiu Danet?
A. Yes.
Q. Based on your review of that hard drive, was there any data useful to further identifying Tiberiu Danet?
A. Yes, there was.
Q. What sort of data did you review that you found helpful?
A. So the hard drive contained a large amount of photos related to travel that Tiberiu Danet took over the long course of a period of time.
Q. How can you tell those were photos related to his travel?

A. Because I could look and see it was in multiple different places as well as he was very meticulous about naming the directories contained in these photos.
Q. Were you able to get any dates or timestamps from those photos?
A. I was, yes.
Q. And based on those, were you able to compare that data with any data you had selected over the course of your investigation?
A. Yes.
Q. And what data did you compare it to over the course of your investigation?
A. I compared it to all the data I had related to activity of one of the e-mail accounts of amightysa to see if there was any correlation between the travel and the activity on that account.
Q. And what sort of data did you review to see about travel from the command and control server to the other search warrant returns?
A. I reviewed data from search warrants, from pen register trap and traces, from Title III, from data intercepts, not only from amightysa but from other accounts that were communicating with amightysa.
Q. And did you, in fact, create a document showing the comparison and analysis of the photos and the search

warrant PRTT data?
A. Yes, I did.
Q. And before publishing to the jury, could you take a look at Exhibit 1849?
(Pause.)
Q. (Continuing) Looking at this, do you recognize this?
A. I do, yes.
Q. How do you recognize it?
A. This is a document I created.
Q. What data did you use to create this?
A. So I used data from search warrants of the amightysa account pen register trap and trace data. I used Title III data on the Master Fraud account as well as data seized from the hard drive at the location associated with Danet in Romania.
Q. And using that data, did you change or modify any of the underlying data?
A. I did not, no.
Q. Is this, in fact, a graph?
A. It is, yes.
Q. And is the graph helpful in organizing a large amount of data?
A. It is.
Q. Does it help you understand the relationship of that

data?
A. Yes.
Q. Does it change the underlying data itself?
A. It does not.
MR. BROWN: Your Honor, I would like to publish Exhibit 1849.
MR. O'SHEA: Your Honor, may we approach?
THE COURT: You may.
(Side bar held on the record.)
MR. O'SHEA: You can see the exhibit right now, Judge, on your screen. I have seen it. What it is, it is an Excel file obviously in native format not converted to PDF.
In that regard, I am not sure how it goes into the jury anyway, number one.
And number two, this idea that this can be an exhibit that summarizes an entire investigation in one Excel sheet does not comply with Rule 106.
THE COURT: Are you asking at this point in time that it be admissible, or is this demonstrative.
MR. BROWN: Your Honor, I am trying to think of his last question first, which is how to go back to the jury.
THE COURT: Well, it does not go back to the jury if it is demonstrative, and I believe Mr. O'Shea is

objecting to admissibility. Am I correct?

MR. O'SHEA: I am objecting right now to even publishing it to the jury.

THE COURT: How is it any different than asking him to go up to a white board and put a timeline on a white board?

MR. O'SHEA: Only in the sense, Judge, that I don't — the general question was: Was the volume of information so great that it would be difficult to present it item by item?

I need a lot more than foundation laid about what information did you use here, not everything you know about the investigation such as, with everything we've heard so far, is this incorporated into this document.

And is there anything that we have not heard yet that is not incorporated into this document for purposes of demonstrative exhibit?

THE COURT: Okay. As of right now, I agree with Mr. O'Shea. This would not be admissible. However, regarding it being demonstrative, I, too, would like more foundation.

But if you do, in fact, establish foundation, I am going to allow it for demonstrative only. So he can use it during his testimony, use it

during closing argument, but I don't believe, as of right now, I don't believe this is an exhibit appropriately admissible.

(Side bar concluded.)

MR. BROWN: Your Honor, is it okay if I stay back here?

BY MR. BROWN:

Q. Special Agent Macfarlane, looking at tab — 1849 is an Excel spreadsheet, correct?

A. It is, yes.

Q. And has multiple tabs?

A. It does.

Q. Okay. I would like to walk you through tab by tab and ask you a few questions?

A. Okay.

Q. Do you recognize which tab we are on right now?

A. I can't see it.

Q. Do you see which tab we are on?

A. Yes.

Q. Okay. And what's the name of that tab?

A. Amightysa log-in data.

Q. And who created the name of that tab?

A. I did.

Q. And from where did you derive that data?

A. I derived this data from legal process associated to

the amightysa account.
Q. What sort of legal process?
A. Subpoenas, search warrant, any legal process associated to that account.
Q. And what is the status showing?
A. It shows the times and dates of when this account was logged into.
Q. Logged into just the e-mail account?
A. Yes. When someone entered a user name and password and logged into the account.
Q. And did you alter that data in entering it into an Excel spreadsheet?
A. No.
Q. Did you change the content of that data?
A. No.
Q. Did you change the format of that data?
A. I did not.
Q. But you entered it into an Excel spreadsheet?
A. You mean the format as the data represented here, yes, but I didn't change the actual — the way the data is formatted in these specific columns.
Q. Moving on to the next tab, do you see this tab?
A. Yes.
Q. And do you see the title of this tab?
A. Yes. It is "amightysa sent e-mail."

Q. By the way, do you know approximately how many lines of data this is, this tab, and if I scroll down, would that help?
A. Yes. So almost 600.
Q. Okay. And where did you get this data?
A. So if you scroll up to the very top, this was from legal process —
Q. Wait. I accidently was hitting page up and typed — okay. Thank you.
Where did you get this data?
A. This data was from search warrants of e-mail accounts associated with the Bayrob Group.
Q. And did you review that data?
A. I did, yes.
Q. And did you change any of that data to put it into the Excel spreadsheet?
A. I did not.
Q. Did you alter any of that data?
A. I did not.
Q. Did you format that data?
A. I did not. I mean, I formatted it for the sheet, but I did not change the format of the specific.
Q. And I don't think I asked you for the prior tab, the information of the prior tab, is that a fair and accurate representation of the log-in data you received via legal

process?
A. It is.
Q. And for the tab named amightysa sent e-mail, is that a fair and accurate representation of the data you received as part of the search warrant data for sent e-mail?
A. It is.
Q. Looking at the next tab, do you recognize this?
A. Yes.
Q. And what is that tab name?
A. This is PRTT log-in data.
Q. And who created that name?
A. I did.
Q. And what does this table show?
A. This shows the results of a pen register trap and trace on amightysa and the log-in events.
Q. Okay. And I am scrolling down.
Do you know approximately how many lines of data this table is?
A. A lot. It is probably 10 — probably 12,000, maybe more, definitely more.
Q. Okay. From where did you get this data?
A. From the provider.
THE COURT: From where?

THE WITNESS: From Google.

BY MR. BROWN:

Q. And what does this data show?

A. It shows log-in events on the — for that account, for activity on that account.

Q. And in fact, do you see the last line?

A. Yes.

Q. And what's the number on that line?

A. 18810.

Q. In receiving this data, did you change any of the data?

A. No.

Q. Did you alter any of the data?

A. No.

Q. Did you modify any of the data?

A. No.

Q. Did you enter it into Excel so it could be analyzed in Excel?

A. I did, yes.

Q. And did doing that modify or change any of the data?

A. No.

Q. Okay. And is this — does this table fairly and accurately represent the PRTT data you received from Google pursuant to this investigation?

A. It does, yes.
Q. Now, going on to the next tab, do you recognize this tab? Let me go up.
A. There was no data reflected in other data.
Q. Okay. Based on all of that data, how did you analyze that data using Microsoft Excel?
A. So I used Excel to compare what I viewed as significant events. So if you are a user of an e-mail account, if you log in or you send an e-mail, you are actively using that account at that time.

So it was a way for me to take data and tie it to an event in the real world, which was just a log-in or a use of this account.
Q. How did you demonstrate that comparison?
A. So what I did is, I created a graph of the events over time.
Q. And what did that graph show?
A. That graph compared multiple points of data for analysis.
Q. And in fact, approximately how many points of data are we talking about?
A. Probably, you know, between 20,000 and a hundred thousand, maybe more.

MR. BROWN: Your Honor, at this time, I would like to publish 1849 as a demonstrative to the

jury.

MR. GOLDBERG: Objection.

MR. O'SHEA: For demonstrative purposes only, no objection.

THE COURT: But Mr. Goldberg, you are lodging an objection?

MR. GOLDBERG: I am still objecting.

THE COURT: Objection not well taken. I will allow it for demonstrative only at this point.

BY MR. BROWN:

Q. Okay. Now Special Agent Macfarlane, could you explain what the tab named "graph" demonstrates?

A. It is a graph of this data.

Q. And who made the name "graph"?

A. I did.

Q. Okay. Now, what specifically does this show? There are lots of colors and names.

A. If you scroll down, there is a key --

Q. Okay. Scroll down.

A. -- on the left.

Q. So is this the key? (Indicating.)

A. It is, yes.

Q. And what do the various numbers represent in this key, colors, I'm sorry. Colors.

A. So the light blue represents log-in data. The orange represents e-mails sent from amightysa. The gray color is -- represents data from the PRTT, and the yellow shows data from the T-III.
Q. Okay. And what is the blue and yellow bottom line?
A. The blue and yellow bottom line is like all the data points.
Q. Now, there are words along the top. What do those represent?
A. The words along the top relate to photos obtained from the hard drive on Danet's apartment -- in Danet's apartment.
Q. And what specific information from the photos do those words represent?
A. The location those photos were taken.
Q. So the countries they were taken in?
A. Yes.
Q. And there are vertical lines, and we will zoom in a little bit that intersect all the lines with a date?
A. Yes.
Q. And what are those dates?
A. That would be the date at that point in time in the graph.
Q. And can you explain, is there a specific date range

that you used for this graph?
A. So I used the — I used the date range of the first data that I had and all the way to the take down of the botnet or the arrest of the — the arrest of Tiberiu Danet, Bogdan Nicolescu, and Radu Miclaus.
Q. And I will start, looks like the date is December 27th, 2014.
Do you see on the left what I am doing? Could you explain what we are looking at in this section or this view of the graph?
A. So we are looking at the — for example, this is the area where the United States is. Those were actually — that was Danet's trip to where he came in through Miami.
Q. So based on this sort of blue collection of blue dot lines, that means he is in the United States?
A. Yes.
Q. And what do the other lines mean?
A. That's where he was at that time.
Q. If you move down one line under the United States, what does that tell you —
A. That's T-III data.
Q. What does that tell you about T-III data?
A. So basically, it tells me there is no activity in the T-III data.

Q. Because if there was, there would be a colored dot?
A. Yes.
Q. And what do the colored dots represent?
A. Like a sent e-mail for a T-III, for example.
Q. If we are still using the United States example, what does it tell you on the gray line?
A. The gray line says that from the PRTT, there was no data sent from the amightysa account.
Q. Okay. And how about this sort of orangish line?
A. That means there was no log in.
Q. And what about the — the orangish line?
A. If you can scroll up to the key.

So the orange line, is that out of search warrant results there was no sent e-mail, and the blue line would be no log in.

Q. Okay. And you did this for how long of a time period?
A. I did this for — if you can scroll to the left, I can tell you what the earliest data was. So our data started in May of '13, but if you scroll to the right — keep going — stop — scroll up. A little bit more. Little bit more, little bit more. Hold it. A little bit more. Perfect.
Q. Oh.

A. So this is when I find this data important because, at this point in time, I have what I would consider very good coverage, like vision into a number of different independent data sources related to the activity on the amightysa account.

So I was able to see e-mails that were sent by amightysa based on our legal coverage of the Master Fraud account, of pen register trap and trace on the amightysa account, and associated log-in data for that account.

So it was a good way to see whether someone was sending e-mail or logging into that account at that time from multiple different independent data sources.

Q. And in fact, do you see any trips Danet took for anyone logged into amightysa?

A. No.

Q. And scrolling to the end, what is the significance of the blue line labeled "takedown"?

A. That's when the individuals were arrested, and the botnet was taken down.

Q. Okay. Now, at the time of arrest, did you review any -- was anything recovered from Bogdan Nicolescu, if anything, that helped ID Nicolescu?

A. Um --

Q. Withdraw that question.

Based on this analysis, based on this data, did you come to a conclusion about the identity of amightysa?

A. I did, yes.

Q. What was that conclusion?

A. Based on this information, based on the data amightysa, there were 13 different trips that amightysa took, and during each one of those trips there was no activity on the amightysa account.

There was no e-mail sent from that account. There were no log ins to that account. There were no presence, which means that for some reason that account was active for that e-mail account.

Q. Now, so at this point in the investigation, you believe your investigation has identified two of the four members?

A. Based on this analysis combined with the other technical information I knew about Tiberiu Danet, I knew that amightysa was Tiberiu Danet.

Q. Okay. Now, did you review items recovered from Defendant Nicolescu at the time of his arrest?

A. Yes.

Q. And during your review, did you find any information that was helpful to your identification of him and his

monikers?
A. Yes.
Q. What I would like to do is show you Government's Exhibit 45. Do you recognize this?
A. I do, yes.
Q. And what do you recognize this to be?
A. I recognize this to be the data from the accounts table of the Xabber application on one Nicolescu's phone.
Q. And a phone was seized at the time of his arrest?
A. It was.
Q. And what kind was it?
A. May I check it?
Q. Yes.
A. It was an Asus phone.
Q. And was the Asus phone imaged?
A. It was.
Q. And was the image a true and accurate copy of the contents of the phone?
A. It was, yes.
Q. And did you review the imaged data?
A. Yes.
Q. And based on the data, did you find any data that was helpful in identifying the identity of any of the remaining monikers?

MR. GOLDBERG: Objection.
THE COURT: Overruled. Yes or no, sir.
THE WITNESS: Can you repeat the question?
BY MR. BROWN:
Q. Was there any information on the Asus phone seized from Nicolescu that helped your investigation identify any remaining members of the Bayrob Group?
A. Yes.
Q. Okay. Looking at Exhibit 45, do you recognize that?
A. Yes.
Q. What do you recognize it to be?
A. I recognize it to be data from — may I correct something?
Q. Yes.
A. This is data from one of Nicolescu's phones. Actually, now, it is from the Asus phone. I'm sorry.
Q. Okay. And how do your recognize that to be data from the phone?
A. I reviewed the phone.
Q. Okay. And did you change any of this data?
A. I did not, no.
Q. Did you modify any of this data?
A. I did not, no.

Q. Did you format any of this data?
A. I pulled the data out so that we could do it in this format.
Q. And is this a fair and accurate representation of the data found on Nicolescu's phone?
A. It is, yes.
MR. BROWN: Your Honor, seek permission to publish Exhibit that?
MR. GOLDBERG: No objection.
MR. O'SHEA: No objection, Judge.
BY MR. BROWN:
Q. And Special Agent Macfarlane, what does Exhibit 45 show?
A. Exhibit 45 shows the Xabber accounts that were on this phone.
Q. And specifically what information about the Xabber accounts on this phone does it show?
A. This shows the user name, password, and server name for the accounts, instant messaging accounts.
Q. Okay. And what were the user names found on this phone that you observed?
A. Obe.m
Q. Okay.
A. And I don't know how you pronounce that but zaietz.

Q. Did either of those user names have any investigative value to you?
A. Yes. The obe.m was a user name that we had seen before.
Q. Okay. Do you recall where you had seen it before in your investigation?
A. I seen it — I had seen this specific user name on Danet's phone that we searched in Miami.

(Side bar held off the record.)

THE COURT: Ladies and gentlemen, we are going to take our luncheon recess. Please remember the admonition.

Please be downstairs, and we will call for you at 1:15. All rise for the jury.

(Luncheon recess taken.)

- - - - -

AFTERNOON SESSION

THE COURT: Please be seated. Mr. Brown, you may continue.

MR. BROWN: Thank you, your Honor.

BY MR. BROWN:

Q. Special Agent Macfarlane, before the break, we were talking about users on an Asus phone. Do you recall that?

A. Yes, sir.

Q. And do you recall what user names we were discussing?

A. Obe.m, o-b-e dot m and zaietz.

Q. And can do you recall who the owner of that phone was?

A. Bogdan Nicolescu.

Q. And why was finding a phone owned by Bogdan Nicolescu with the user name obe important to your investigation?

A. Because it confirmed evidence acquired in Miami.

Q. Did you see the user name obe anywhere else?

A. Yes.

Q. I would like to show you Exhibits No. 23 published before we show it to the jury -- or I'm sorry. Just pull up before we publish it to the jury.

And do you recognize this?
A. Yes.
Q. How do you recognize it?
A. This is a screenshot that was found in the phone.
Q. And is this an accurate copy of the screen shot found in — do you know in which phone this was found?
A. I believe the one we were just talking about.
MR. GOLDBERG: Objection.
THE COURT: Was there an objection?
MR. GOLDBERG: Yes, to the form of the question.
THE COURT: Rephrase.
BY MR. BROWN:
Q. Based on your investigation, do you recall which phone this was seen on?
A. Let me just confirm. It is — I am almost positive it is the Asus phone.
Q. Is this a fair and accurate copy of the screenshot of the Asus phone?
A. Yes.
Q. And when I say the Asus phone, is that the Asus phone found in possession of Bogdan Nicolescu?
A. Yes.

Q. Have you changed any of the data on the screen?
A. No.
Q. Is this a fair and accurate representation of the screen when you searched it?
A. Yes.
MR. BROWN: Permission to publish to the jury?
MR. GOLDBERG: No objection.
MR. O'SHEA: No objection.
THE COURT: Did you say objection or no objection?
MR. O'SHEA: I'm sorry. No objection, Judge.
THE COURT: Thank you.
BY MR. BROWN:
Q. And what does this show, Special Agent Macfarlane?
A. This shows a view of the Xabber application on this phone.
Q. Okay. And in fact, how do you know this is the Xabber application on Bogdan Nicolescu's phone?
A. The data is consistent in the screenshot with the underlying data.
Q. The is this Xabber spelled as it normally is?

A. Yes.
Q. Do you recall testifying that Xabber is spelled X-a-b-b-e-r?
A. Yes.
Q. And is that X-a-b-b-e-r?
A. Yes. The one difference on the screenshot at the time this was taken from my analysis of this there was only two accounts, and the database had three.
Q. And what database was this drawn from?
A. The Xabber database.
Q. And was that database on the phone?
A. Yes.
Q. How was seeing that helpful to your identification of Nicolescu?
A. Seeing this image confirmed to me that Nicolescu did, indeed, use the moniker obe.m.
Q. And did you see any other device — did you review any other devices that had conversations with obe.m on them?
A. Yes.
Q. Okay. Can I show you Exhibit 185? I believe that's a telephone.

THE COURT: Jurors — can the jurors see it?

MR. BROWN: It should be a typical phone.

THE COURT: You said 185?
MR. BROWN: 185, yes, your Honor.
BY MR. BROWN:
Q. Did there come a time when you reviewed an image of a telephone of Radu Miclaus?
A. Yes.
Q. And do you recall what type of telephone it was?
A. A Huawei.
(Discussion held off the record.)
THE COURT: Please be seated. I apologize Mr. Brown.
MR. BROWN: Not at all. Thank you very much.
BY MR. BROWN:
Q. I would like to show you — show you Government's Exhibit 185.
MR. BROWN: Permission to approach the witness?
THE COURT: Of course.
MR. BROWN: Thank you.
BY MR. BROWN:
Q. Do you recognize this?
A. Yes.
Q. What do you recognize that to be?

A. Evidence Item 1 B 20 underscore 12.
Q. And how do you recognize that item?
A. Because it is marked that item on the back.
Q. What specifically do you recognize that item to be?
A. This is a Huawei phone seized from the person or car of Radu Miclaus.
Q. And was a forensic image of that phone made?
A. Yes.
Q. And did you review the forensic image of that phone?
A. I did, yes.
Q. Was there anything on the forensic image of that phone useful to your investigation?
A. Yes.
Q. Was there anything useful on that phone to identifying Radu Miclaus?
A. Yes, there was.
Q. Was there anything useful in identifying Bogdan Nicolescu?
A. Yes, there was.
Q. I would like you to look at Exhibit 232 without publishing to the jury first. Do you recognize Exhibit 232?
A. I do, yes.

Q. How do you recognize that?
A. I recognize it because I recognize the data within it and the table the data came from.
Q. Where did you find the data in Exhibit 232?
A. In a table related to the Xabber application called accounts.
Q. And where was that table located?
A. It was in the Xabber database.
Q. On — was it on a computer —
A. It was on the phone.
Q. On the phone you just testified about?
A. Yes.
Q. And did you create any of this data?
A. No.
Q. Did you modify any of the data?
A. No.
Q. Did you format any of the data?
A. I formatted it for viewing, yes.
Q. In formatting for viewing, did you change any of the data?
A. No.
Q. Is this a fair and accurate representation of the data that was imaged from Miclaus Huawei phone?
A. Yes.

MR. BROWN: Your Honor, at this time I would

like to publish Exhibit 232.

MR. GOLDBERG: No objection.

MR. O'SHEA: A moment please, Judge?

THE COURT: Sure.

(Pause.)

MR. O'SHEA: One moment, please. Just a little longer.

THE COURT: Sure.

(Pause.)

MR. O'SHEA: No objection, Judge.

MR. BROWN: Permission to publish, your Honor? Sorry. Thank you.

BY MR. BROWN:

Q. And what information on Exhibit 232 was helpful in your investigation?

A. So the information on Exhibit 232 that was helpful were the user names, passwords, and server names associated with furty 2 mobile.

Q. And why was the user name furty 2 mobile to your investigation or furty 2 mobile? I'm sorry.

A. So I had seen a user name containing furty in locations within the investigation, specifically Danet's phone, which was imaged in Miami.

Q. Did you find any evidence that furty 2 mobile was the user name used in applications on this phone?

A. Yes. That's what this data would represent in this location.
Q. Were you able to review any of the Xabber chats on this phone?
A. Yes.
Q. And were any of the chats you reviewed on this phone useful to your investigation?
A. Yes, it was.
Q. What I would like to do now before publishing is show the witness Exhibit 227, and do you recognize this?
A. I do, yes.
Q. And how do you recognize it?
A. It was a screenshot obtained on this phone.
Q. And how do you recognize it to be a screenshot on that phone?
A. I recognize it from the screenshot on the phone as it was found on the phone.
Q. Did you add any data to this screenshot?
A. I did not.
Q. Did you change any of the data from the screenshot?
A. I did not.
Q. Did you modify or format this image?
A. No. This was how it was found on the phone.

Q. And is this a fair and accurate representation of the screenshot imaged from Miclaus phone?
A. Yes.
MR. BROWN: Permission to publish 227, your Honor.
MR. GOLDBERG: No objection.
MR. O'SHEA: No objection, Judge.
BY MR. BROWN:
Q. And taking a look at Exhibit 227, could you explain what you saw in this screenshot?
A. So based on my investigation, I had come across a number of Xabber accounts on a number of different phones, and those Xabber accounts came — were related to handles like user names that were common across those phones, and they came in two varieties.
They came in the mobile variety where there would be an indicator like .m or mobile and just the plain variety, which would be a user name.
Based on other information obtained during the investigation, I was able to determine that those user names were associated with —
MR. O'SHEA: Objection.
THE COURT: Overruled.
A. — a Jabber account on a mobile device and non mobile device.

Q. And based on that investigation, could you determine who obe@aro.strangled.net was?

MR. GOLDBERG: Objection.

THE COURT: Overruled.

THE WITNESS: Bogdan Nicolescu.

BY MR. BROWN:

Q. And could you determine who he was communicating with in this screenshot?

A. Radu Miclaus.

MR. O'SHEA: Objection.

THE COURT: Overruled.

BY MR. BROWN:

Q. And could you determine the content of this information?

A. Yes, once it was translated.

MR. BROWN: Your Honor, could we pull up Exhibit 243, just page 19? I'm sorry, page 2.

MR. O'SHEA: Did you say 249?

MR. BROWN: No, no. Exhibit 243, and go to page 19.

BY MR. BROWN:

Q. Okay. Could you take a look at page 4 of Exhibit 227? Is this a translation on the right?

A. Yes, it is.

Q. And did you review the translation?

A. I did.
Q. What in the translation was useful to your investigation?
A. The content of the message led me to believe they were talking about money.
Q. Was anything in this conversation helpful in linking identities with user names?
A. Yes.
Q. What?
A. The letters MF and the letters Min.
Q. And in reading this conversation, could you tell who MF was and who min was?
MR. GOLDBERG: Objection.
MR. O'SHEA: Objection.
THE COURT: Overruled.
A. In this conversation, I could understand that obe at aro.strangled.net was sending this information related to Master Fraud and related to Minolta to Bogdan Radu Miclaus.
Q. And based on this screenshot, were you able to make conclusions about the identity of Bogdan Nicolescu?
MR. GOLDBERG: Objection.
MR. O'SHEA: Objection.
THE COURT: Overruled. Yes or no, sir.
A. Based on my review of this data and other data, I

came to the conclusion that Bogdan Nicolescu --

MR. O'SHEA: Objection.

THE COURT: Sustained.

BY MR. BROWN:

Q. Based on your review of searched warrant e-mail data, T-III intercepted data, and this screenshot, were you able to make an identification of who MF was?

A. Yes.

MR. GOLDBERG: Objection.

THE COURT: Overruled.

A. Based on my knowledge of the active members of the Bayrob Group and the identifications that had previously been done combined with the data contained on this phone, I was able to identify Bogdan Nicolescu as Master Fraud.

Q. Based on the evidence you collected during your investigation, were you able to understand the roles each of the three of the four members of the Bayrob Group played?

A. Yes.

Q. And based on your review of the evidence you collected during your investigation, were you able to determine what role Bogdan Nicolescu played?

MR. GOLDBERG: Objection.

A. Yes.

THE COURT: Sustained.

BY MR. BROWN:

Q. During the course of your investigation, were you able to identify where computers infected with the Bayrob Trojan were located?

A. I did, yes.

Q. And were you also able to determine when the computers were infected?

A. Yes.

Q. How did you keep track of the name of the victim, location of the victim, and the approximate date of the infection?

A. The Bayrob Group kept extremely good records of all of the records within their database.

Q. Based on those records, were you able to create any data to help yourself keep track of these dates, times, and locations?

A. Yes, I was.

Q. And did you create a table with that information?

A. I created multiple tables, yes.

Q. Is the table you created about the name of the victim, location of the victim, and approximate date of the infection in the indictment?

A. Yes.

Q. Okay. I would like to show you a table from the indictment.

MR. BROWN: This is for demonstrative.

MR. O'SHEA: Not published yet, right?

MR. BROWN: Not published yet.

MR. O'SHEA: What exhibit is it?

MR. BROWN: Page 28 and 29 of the indictment.

BY MR. BROWN:

Q. And this is a two-page table?

A. Yes.

Q. And did you create this table?

A. I did.

Q. Based on what information did you — what information did you use to create this table?

A. I used information that was kept by the Bayrob Group to create this table.

Q. Where was that information kept?

A. It was on the command and control servers in the database.

Q. Approximately how many files did you review to create this table?

A. To create this specific table?

Q. Yes.

A. I believe this was all in one — one database.

Q. And how large was that database?
A. Over 50 tables large. I don't know exactly what the size of that database was.
Q. Did you create this table as a way to help organize the data —
A. Yes.
Q. — and to make it more reviewable?
A. Yes.
Q. Did you change any of the data in this table?
A. No.
Q. Did you alter any of the data in this table?
A. No. I did change the victims. We abbreviated their names.
Q. Did you change them or abbreviate them?
A. Abbreviate them.
Q. Okay. But do the abbreviations accurately reflect the names of the victims?
A. Yes.

MR. BROWN: Your Honor, permission to publish to the jury?

MR. O'SHEA: Objection, your Honor. May I have a side bar?

THE COURT: Yes.

(Side bar held on the record.)

MR. O'SHEA: This is unconditionally

hearsay, period, based on hearsay, period, period. That's my objection. It dovetails right -- and if it is not hearsay, then it is Crawford based stuff, period.

MR. BROWN: We are not offering this as admission but as a demonstrative drawn from data from the command and control server, which are -- was created by party opponents. It is not hearsay.

This is just to summarize certain facts learned in the investigation. We were not asking to admit it, and we are not even asking to have this table sent back to the jury.

As with the other table earlier in the trial, this is the same demonstrative with the understanding of its limited use as a demonstrative, and it was by agreement of the parties.

THE COURT: What was by agreement of the parties?

MR. BROWN: That we are sending the indictment back but not these tables.

MR. O'SHEA: Understood. However -- here is what I anticipate in closing. "Ladies and gentlemen, you" -- showing them the indictment in closing -- "here is what the witness testified to on the stand."

It is demonstrative. They get to show it. It is another way of end-rounding the whole thing.

MR. BROWN: No.

MR. O'SHEA: I understand what their complexities are, but I have to object.

THE COURT: Okay. This exhibit is taken right from the indictment. Am I correct?

MR. BROWN: Yes.

THE COURT: And you want him to testify that the chart in the indictment is basically everything he saw in the data?

MR. BROWN: No. It is a summary of infected computers in the Northern District of Ohio on a certain day — on certain dates that he saw in his review of data, computers in Ohio infected on those dates with the victim name obviously changed or initials.

THE COURT: So if he — he is an expert. He had reviewed all of the data, and he is simply going to testify that he saw the first item in the table, in the data. How is that hearsay?

MR. O'SHEA: Well, I assume it is in lieu of having the actual victims come in here and testify as individuals that they were victimized or anything like that.

And they are going to argue that one of this is just part of the conspiracy. Therefore, they are all in for the conspiracy. It is kind of wedging the whole

thing in, Judge. I am uncomfortable with it from a Crawford basis.

THE COURT: Well, unfortunately, I think you are going to have — unless there is an agreement, I think you do have to go through each one and say how he arrived at — including that one, which means you are going to have to go through the data. Look — of course, you can talk.

(Discussion held off the record.)

THE COURT: Folks, feel free to stand and stretch. That should be a given.

(Pause.)

(Side bar continues.)

MR. O'SHEA: I think we have resolved it, your Honor.

THE COURT: How are you going to resolve it?

MR. O'SHEA: For the record, I said, based upon the explanation I am getting about what questions he is going to ask and in order to move it along, because it is voluminous, I said he could lead the witness a little bit, but I just want to be very careful when we start doing it that there are no conclusions made by the witness about what it all means.

THE COURT: Okay. Fair enough.

MR. BROWN: And I ran through questions that I was going to ask.

THE COURT: Okay.

(Side bar concluded.)

BY MR. BROWN:

Q. Looking at this table, did you review the data collected from wires and search warrant returns to identify infected computers in the Northern District of Ohio?

A. Yes.

THE COURT: May the jury see this?

MR. O'SHEA: Not yet.

THE COURT: Not yet. Go ahead.

BY MR. BROWN:

Q. And based on that review of the data, were you able to identify infected computers, their location, and approximate date of infection?

A. Yes, I was.

Q. And based on the review of that data, were you able to collect that data and put it in a table?

A. Yes, I was.

Q. And was that table created in order to make it easier to organize data related to the Northern District of Ohio?

A. Yes.

Q. In that table, did you create any of the data that you drew from?
A. No.
Q. Did you modify any of the data from the command and control servers or search warrant affidavits or returns?
A. For this table, the only modification that was made was that I shortened the names into abbreviation, but the data contained in the original databases that this came from contained their actual name.
Q. And is the table you created a fair and accurate representation of the data you reviewed that showed the date, victim or name of the computer, and the approximate date of infection?
A. Yes. The data contained on the command and control server to my knowledge was accurate.
MR. BROWN: And your Honor, at this time, I would like to publish the table.
THE COURT: Mr. Goldberg?
MR. GOLDBERG: No objection.
MR. O'SHEA: No objection, your Honor.
BY MR. BROWN:
Q. And in fact, does this table show the location of an infected computer?
A. I don't have it.

MR. BROWN: It is back here on the big TV.
A. For some reason —
MR. BROWN: May I approach the witness?
A. There it is. I have it now.
MR. BROWN: Very dramatic today, your Honor.
BY MR. BROWN:
Q. Do you recognize this table?
A. Yes.
Q. Okay. Is this the table you created?
A. Yes.
Q. And does it show the location of an investigated computer on a certain date?
A. Yes.
Q. Okay. Now, if we could without publishing to the jury show a second table.
Did you also review the data on the command and control server and wire intercept returns to identify computers infected — infected computers with the miner force program in the Northern District of Ohio?
A. If you are asking if this table represents victims in the Northern District of Ohio that were involved in cryptomining —
Q. Yes.
A. — yes.
Q. Okay. And to create this table, what data did you

review, what locations of data, search warrant data?
A. Yes.
Q. Wire data?
A. Yes.
Q. And the data you reviewed, did you change the data when creating your table?
A. No.
Q. Did you modify the data when using your table?
A. No.
Q. Did you alter the data in any way when creating your table?
A. No.
Q. Did you format it to put it in a table?
A. Yes.
Q. Okay. Was the data that you identified based on the Northern District of Ohio part of a larger set of data?
A. Yes.
Q. By putting it into the table, was it easier to understand and organize based on the location of the computer?
A. Yes.
Q. Okay. Is this a fair and accurate representation of the data table you created?

A. It is, yes.

MR. BROWN: Your Honor, permission to publish this to the jury?

MR. GOLDBERG: No objection.

MR. O'SHEA: No objection.

BY MR. BROWN:

Q. And in fact, is this a table you created?

A. It is, yes.

Q. And does it show a victim ID number?

A. It does.

Q. Did you create that name, or is that taken from the data?

A. That was taken from the database.

Q. And does it also show location of an infected computer?

A. It does, yes.

Q. And did you identify each of these places within the Northern District of Ohio?

A. I did.

Q. And did you also do that with the previous table?

A. I did.

Q. And was your analysis of the data able to identify an approximate date of the cryptomining event?

A. Yes.

Q. And is that reflected in the final table or the

final column?
A. Yes.
Q. Okay. And is this a two-page -- and are these also part of that same table?
A. Yes.
Q. And then, finally, based on your review of the T-III data and search warrant data -- I'm sorry.
Going back to that table, were these dates between the years 2013 and 2015?
A. Can I see the second half of the table?
Q. The second page.
A. Yes.
Q. And likewise, could you put the previous table up? Are these dates between 2013 and 2015?
A. Yes.
Q. Finally, did you review the wire data and search warrant data to identify when domain names were registered by the Bayrob Group?
A. I did.
Q. Viewing that data, were you able to identify based on date, certain dates when domain names were registered by the Bayrob Group?
A. I was, yes.
Q. And based on your review of the data, were you able to identify domain names that were used using stolen

credentials or stolen credit cards?

MR. O'SHEA: Objection.

THE COURT: Overruled.

A. I was able to identify domain names that were registered using stolen credit cards, yeah.

Q. And based on that review of the data, were you able to create a table demonstrating the dates that domain names were registered using stolen credit cards or stolen credentials?

A. Yes.

Q. And using the dates, were you able to create sort of subsets of information that were part of a larger block of information?

A. Yes.

Q. And were you able to create a table reflecting a certain date range showing when domain names were registered using stolen credentials?

A. Yes. I would have the dates or approximate dates.

Q. And did you, in fact, create a table using that data?

A. I did.

Q. Was the data you used to create that table modified by you in any way?

A. Not that I am aware of, no.

Q. Was it changed in any way?
A. Not that I am aware of, no.
Q. Did you do anything to the names that you might have found?
A. No. It would be data from the search warrant data.
Q. Okay. Well, directing your attention to the first table you made where you —
A. No. I never changed any data.
Q. Did you use initials for people's names?
A. Other than — yes, like shortening names into initials.
Q. Did you format this data in a way that would be easy to read or understand?
A. I did, yes.
Q. In creating that format, did you change or alter any of the data?
A. No.
Q. Okay. Could you take a look at page 45, 46, 47 without publishing it to the jury? Do you recognize this?
A. Yes.
Q. Is this, in fact, the table you made or the first page of the table you made?
A. Yes.

Q. Is this the second page?
A. Yes.
Q. And is this a third page?
A. Yes.
Q. Okay.
MR. BROWN: Permission to publish to the jury, your Honor?
MR. GOLDBERG: Objection.
MR. O'SHEA: No objection.
THE COURT: Did you say objection?
MR. GOLDBERG: Yes.
THE COURT: Similar to what we already discussed?
MR. GOLDBERG: Yes.
THE COURT: I am going to allow it over objection.
BY MR. BROWN:
Q. Okay. And does this table represent the registration of a domain name using stolen credentials or credit cards?
A. It represents, yes, domains that were registered using stolen information, and yes, stolen credit card information obtained by the Bayrob Group.
Q. And does this table represent registration of domain names during the year of 2014?

A. Yes. There is registrations during 2014.
Q. And Special Agent Macfarlane, based on the totality of your investigation and your review of wire data, pen trap and trace data, search warrant data, chat logs and seized evidence, were you able to identify an individual who used the name or used the moniker Master Fraud?
A. Yes.
Q. And who was that?
MR. GOLDBERG: Objection.
THE COURT: Overruled.
THE WITNESS: Bogdan Nicolescu.
BY MR. BROWN:
Q. And were you able to identify an individual based on the totality of your investigation, the review of search warrant data, wire data, and seized evidence to identify an individual who used the moniker Minolta 9797?
A. Yes, based on the totality of my investigation.
Q. And who was that?
MR. O'SHEA: Objection.
THE COURT: Overruled.
A. Radu Bogdan Miclaus?
MR. BROWN: Thank you. No further questions for this witness.
THE COURT: Thank you. Cross examination, Mr. Goldberg?

CROSS EXAMINATION

BY MR. GOLDBERG:

Q. Good afternoon, Agent Macfarlane.

A. Good afternoon.

Q. You have been referring to notes up there during your testimony.

What are you looking at?

A. I am looking at notes that I put together for data from my investigation, from all the search warrants that I served, all the wire, the intercepts, the data intercepts that were done, and it is just sort of a — I would summarize it as a highlight, highlights of the investigation.

Q. And you used it to refresh your memory during the course of your testimony?

A. Yes.

Q. All right.

MR. GOLDBERG: I make a motion pursuant to Rule 612 we be able to inspect his notes, your Honor.

But in the meantime, I will ask questions.

THE COURT: You don't want to do it now?

MR. GOLDBERG: I want to ask a couple questions.

THE COURT: Go right ahead.

BY MR. GOLDBERG:

Q. Special Agent Macfarlane, you heard Tiberiu Danet yesterday, correct?

A. Yes.

Q. And he was asked questions by myself about his meeting with you and Special Agent Diaz at the FBI offices sometime last summer, correct?

A. Yes.

Q. And you were in attendance at those meetings, correct?

A. I was.

Q. And this was the first time you had a chance to actually talk to somebody that you believe was in the core of the Bayrob Group, correct?

A. Yes.

Q. So I am sure you had a lot of questions for him, specific questions, right?

A. I did, yes.

Q. And it is important to take good notes of the answers to those questions, right?

A. Yes.

Q. You don't use a tape recorder; you rely on written notes?

A. Yes. Notes are important, absolutely.

Q. And both you and Special Agent Diaz took notes at

that meeting, correct?
A. I know that I took notes, yes.
Q. Okay. Well, you know what a Form 302 is, correct?
A. Yes.
Q. So I am going to hand you what I am going to mark as Defense Exhibit O and ask you if you can identify it.
Just ignore all the writing on it. That's from me.
A. Okay.
(Pause.)
A. Yes, I recognize this 302.
Q. And go through it. Have you had a chance to review it?
A. A portion of it, yes.
Q. Okay. So you would agree with me that who was using the moniker Master Fraud is of — the key issue in this case as far as my client is concerned?
MR. BROWN: Objection.
Q. Correct?
THE COURT: Overruled. You may answer that.
THE WITNESS: I think it is a very important question, yes.

BY MR. GOLDBERG:

Q. And in fact, that was one of the last questions you were asked after about six hours of testimony just now, correct?

A. Yes.

Q. And you had just testified that the thing that kind of — decided it for you or the straw that broke the camel's back in deciding the identity of Mr. Nicolescu were the Jabber messages we saw in recently Exhibit 237, I believe, correct?

A. The data contained within the Jabber messages was one aspect of the case that pointed towards Nicolescu, yes.

Q. Okay. But I think you were asked a question: Were you able to identify who obe was and Master Fraud from those messages, correct? Do you remember that a few minutes ago?

A. Yes.

Q. And you said yes, and based on this and everything else, Nicolescu is Master Fraud, right?

A. Yes.

Q. Your investigation was centered for years in finding out who Master Fraud was, right?

A. Yes.

Q. And when you sat down with Mr. Danet in July of last

year, did you ask him who Master Fraud was?
A. No. I told him who Master Fraud was.
Q. Where in the notes does he confirm who Master Fraud was?
A. I didn't need him to confirm.
Q. Well, he confirmed other people's identities, right?
A. Yeah, yes.
Q. Yes, confirmed identities of other persons, correct?
A. That is correct.
Q. All right. So you didn't think it was of investigatory significance for you to say "is Nicolescu Master Fraud?" You never asked him; you just told him?
A. I confirmed it with him.
Q. Why isn't that in your notes?
A. Because I already knew who Master Fraud was.
Q. Do you only put in what you don't know into your notes?
A. I put what I need to remember, and I would remember that Nicolescu was Master Fraud.
Q. Okay. Well, you know, I appreciate your explanation, but the whole point of the 302 is

to —

MR. BROWN: Objection.

THE COURT: One moment. The beginning statement will be stricken.

Please ask a question.

MR. BROWN: Thank you, your Honor.

BY MR. GOLDBERG:

Q. What's the reason for having a 302 to create that document?

A. Having a 302 documents an interaction.

Q. Okay. And don't you think it is important if there is a discussion regarding the ultimate issue in a serious criminal case that you have been investigating for five or six or seven years, that you put it in that document?

A. All I can say is that I wrote the 302 based on the interaction.

Q. Okay. Well, yesterday Danet said "oh, I said that Nicolescu was Master Fraud." Do you remember that?

A. Yes.

Q. Well, he must have been lying because you said you told him.

MR. BROWN: Objection.

THE COURT: Sustained.

BY MR. GOLDBERG:
Q. Was that true, did he tell you that?
MR. BROWN: Objection.
THE COURT: Overruled.
BY MR. GOLDBERG:
Q. Did he tell you that Nicolescu was Master Fraud?
A. Yes. He confirmed that Nicolescu was Master Fraud.
Q. Okay. But that was not written down in your 302. We can agree on that?
A. Not this 302, no.
Q. Okay. Do you remember yesterday — one more question on the 302:
Mr. Danet testifying about whether or not he knew who Matei Marius was, do you remember that line of questioning?
Do you remember him saying — he put it this way: Do you remember him saying he doesn't know who he was?
A. I can't recall that specific aspect of yesterday's testimony.
Q. Fair enough. I will take that back. Thank you.
In 2015, in June, you were able to conduct your or execute the search warrant on Mr. Danet's phone at the Miami airport, correct?

And I am not trying to trick you about the date.

MR. BROWN: Objection.

Q. Whenever he was any of Miami.

A. Yeah.

THE COURT: Overruled.

Q. It was May?

A. May, yes.

Q. May 15th, right?

A. Around that.

Q. Okay. So you got the phone, and you were able to copy it, right?

A. That's correct.

Q. And are you familiar with cellphone operating systems?

A. Like Android or OS X or — yeah.

Q. Exactly.

A. Yes.

Q. Exactly?

A. Yes.

Q. Okay. And are you familiar with the term "jail broken phone"?

A. Yes. I am familiar with that.

Q. What does that mean?

A. A jail broken phone is a phone where the operating

system has been modified so that you can do — you can have additional capability with the phone.

Q. And did you fine that Mr. Danet's phone was jail broken?

A. I don't recall at this point in time.

Q. Did you happen to look?

A. For this specific phone, I don't know. I reviewed a lot of phones for this case.

Q. Okay. But if a phone has the jail broken capabilities that you have just defined, it can operate other applications or multiple — multiple copies of an application at one time, correct?

A. It is a possibility that that jail broken phone can multitask, but I believe that other phones can multitask as well. I don't know if that's a feature only of a jail broken phone.

Q. But you would agree with me that Mr. Danet had some pretty high skills, basically had a Master's Degree in computer science?

A. Mr. Danet?

Q. Yes.

A. Yes.

Q. The person whose phone was taken?

A. Yes.

Q. And if there was, if there was a capability of

manipulating the phone, he had the skill set to be able to do that?

MR. BROWN: Objection.

THE COURT: Overruled. Can you answer that, sir?

A. I don't know if Danet had the capability to modify the Android operating system, but what I do know is, I didn't see any indication of it.

Q. Okay. Did you see an indication that he was carrying on multiple conversations or chats on his phone over multiple platforms?

A. Yes. I would say that's true.

Q. Now, you were at some point during your testimony asked about the search of Danet's home, and that occurred in September 2016, and certain items that were seized?

A. Yes.

Q. Do you recall whether the server that housed or hosted the Jabber application that we heard about from Mr. Danet, whether that machine was seized by the FBI or by the Romanian Police and turned over to the FBI?

A. So I was not at the location, so I didn't directly witness what occurred there and what was seized.

All I can say was that there was a log made of that location by the Romanian National Police.

Q. Let me ask you this: The Jabber chats are of major significance to your investigation, Jabber chats that Danet had with members of the conspiracy, other people that haven't been named in the conspiracy, correct?
A. That is correct.
Q. And I would imagine, then, that a forensic copy was made of the Jabber server so that the integrity of that system could be tested and reviewed by both law enforcement and the defense?
A. So what I do know is I didn't review a server that contained Jabber chats. The only devices that I reviewed that contained Jabber chats were phones.
Q. Okay. But you knew early on that that server was physically located in Danet's house or apartment, right?
A. No.
Q. All right. But at some point, you knew that?
A. The only thing I knew about Jabber relating to Danet's house was that there was Jabber traffic going to Danet's house.
Q. Okay. But when he proffered and talked to you, he told you that he had the server at his house?
A. I would have to review the proffer.
MR. GOLDBERG: May I approach, your Honor?

THE COURT: You may.
THE WITNESS: Do you know what page it is on?
BY MR. GOLDBERG:
Q. Yeah. I think it is later.
A. In this proffer, he stated that he did not set up the Jabber server in his house for criminal activity.
Q. Okay. But he did indicate to you that he had the Jabber server at his house?
A. Yes.
Q. And is it fair to say that, if you have got the server, you can see when the individual device is signed on?
MR. BROWN: Objection.
THE COURT: Overruled.
A. It would depend on the configuration of the Jabber server, whether it was logging that specific data.
Q. So it would depend on the configuration?
A. Yes. So I know that you can set up Jabber servers to log or not log.
Q. Okay. But we don't know how this was configured because it was never analyzed by the FBI as far as you know?
A. As far as I know, no, I don't believe this was. That being said, there were encrypted devices found

within that — within that residence.
Q. Okay. All right. But let's say that the Jabber server was configured to keep a log —
A. Yes.
Q. — of which user names, which passwords, which devices attached to those user names and passwords were using the server to communicate and at what times that you would have that information. But if it is not set up to keep — to make a log, you wouldn't have that information?
MR. BROWN: Objection.
THE COURT: Overruled.
A. Yeah. If it was set up to log, certain data points would be kept. As far as the devices, the specific devices, I am not a hundred percent sure that device is the right term. It would more likely be —
Q. A sim card.
A. No, like it would be — you know, it might log the type of client coming in or it might not.
Q. Okay. But if I would have logged on with my phone under obe.m to the server at Mr. Danet's house, if it was keeping a log, we would know that Michael Goldberg logged in and not somebody else?
MR. BROWN: Objection.
Q. Because that would come back to a device that I

owned, correct?

THE COURT: Overruled.

A. I don't believe that's true. I don't believe the logging would get that specific for that device. I believe you would need other steps to be able to determine that connection.

Q. We just heard a whole lot of evidence on your direct about things you were able to mine out of the servers and out of the returns from the search warrants and everything else and able to paint a very clear picture of how you think the Bayrob conspiracy operated, correct?

A. Correct, yes.

Q. And I know you have been doing this kind of work for 15 years, and I know that you can identify, at least, some characteristics of a device that is used to log on to a server, if not the name, the operating system or some other identifying characteristic. Isn't that correct?

MR. BROWN: Objection.

BY MR. GOLDBERG:

Q. Was there operational -- there was no reason to not look at the Jabber server that you took out of Mr. Danet's house as part of this investigation. It just didn't get done.

A. I still don't think that we established that there was a Jabber server in Danet's house at the time that the arrest was that was in a state that was reviewed.
Q. Well, he certainly said there was in his testimony.
A. In the review of the evidence that I looked at, I didn't see one.
Q. Could he have been lying?
MR. BROWN: Objection.
THE COURT: Sustained.
BY MR. GOLDBERG:
Q. Let's be clear:
The Jabber platform itself is not necessarily a secure format in that if you have got the user name and you have got the password, you can log on under that —
A. Yes. If you have the user name and password, you have access to that account.
Q. And we can agree, when I asked Mr. Danet that question, he said the same thing, you could log on, correct?
A. Yes.
Q. And I asked him as the system admin — I asked him if he was the system administrator of the Jabber, correct?
A. Yes.

Q. And he said he was. And I asked: Would you have access to the log-on credentials to any of the users? You remember what he said?
A. I believe he said yes, as well.
Q. And so wouldn't the FBI want to know that if evidence that you are going to rely on and you are going to hold up as the key evidence identifying Mr. Nicolescu as actually mirrored on a device that was in your possession, that the witness says contained that information?
A. If we were able to access that data, yes, that would be great.
Q. Did you try?
A. Yes.
Q. You tried?
A. Yes.
Q. Okay. Where is that noted in your file, that you tried to access the Jabber server?
A. I tried to access data that I could not get to as was found both in the documents and worked with other aspects of the FBI. So we were trying to get into the encrypted partition.
Q. The encrypted partitions at Mr. Danet's house?
A. Yes.
Q. So it may have been there, but it may have been

encrypted. You don't know?
A. I don't know.
Q. Well, did you ask Mr. Danet when you proffered him twice?
A. Yes. And he provided credentials to get into the LUKS partitions as well as to get into additional partitions.
Q. Okay. That's a good place to go. So he got password he gave you passwords. He gave you a whole list of them, correct?
A. Yes. He gave us —
Q. And I understand there is not like giving a password like your dog's name; it is more complicated than that, and you can explain that if you want.
A. Yes. So effectively, there were, at least, levels of encryption as described by Mr. Danet.
Q. Okay. And as part of this proffer, he had given you passwords, any and all passwords, correct? He have had to?
A. Yes.
Q. And he told you he had somewhere encrypted in his machines up to 200 bitcoins possibly?
A. Yes, around that amount.
Q. Which he is supposed to proffer, I'm sorry, which he is supposed to forfeit as part of his plea deal in this

case?
A. Yes.
Q. Okay. How much is a bitcoin worth right now? Do you know?
A. Estimated about $5,000.
Q. So if you had 200 of those, what does that come out to?
A. 200 times 5,000? $500,000. No, I'm sorry. It is a million dollars.
Q. That's what I was thinking. I didn't want to say it.
A. It has been a long day.
Q. Okay. So it is about a million dollars that he is saying he has in his computer, but he can't come up with the password, correct? Isn't that correct?
A. That's correct. He was not able to tell us the correct password.
Q. So he gave you some passwords, got you somewhat into the LUKS partition, right?
A. Yes. He got us into the first layer of the encryption.
Q. Okay. And — but the other layers remain encrypted, and you can't get in them?
A. No. We cannot at this point.
Q. Even though that million dollars potentially is part

of Mr. Danet's deal —

MR. BROWN: Object.

Q. — that he made with the Government?

THE COURT: Overruled.

A. Yes. The million dollars we would love to be able to access that million dollars, so we could take that money and attempt to make some of the victims in this case whole.

Q. Of course.

A. Mr. Danet will never see that, no.

Q. Well, maybe Mr. Danet won't see it, but presumably if Mr. Danet was hiding the passwords and gave them to somebody else, they could get that bitcoin, correct?

MR. BROWN: Objection.

Q. If you had —

THE COURT: Overruled.

A. If they were able to access the encrypted partition that contained the wallet —

Q. Correct.

A. — and knew whatever — and again, knew the credentials to that wallet, yes, they would be able to. But I don't intend to provide that to anyone.

Q. Well, let me ask you something. In your 15 years at the FBI, have criminals buried anything in their backyard or hidden the loot somewhere so if they get arrested

someone else can get it for them?
A. Sure.
Q. So isn't the same thing doable with regard to this bitcoin?
A. Potentially, yes. Potentially, it is.
Q. So potentially, Mr. Danet can make the deal, get the credit, tell on his friends, get out in nine or 12 years and go to Switzerland and pick up his million dollars, right, potentially?
MR. BROWN: Objection.
THE COURT: Sustained.
BY MR. GOLDBERG:
Q. All right. So during the course of this investigation, you were able to access — you had a Title III, a pen register or search warrants would you say to cover the entire period from 2013 to the arrest date, or were there breaks in your surveillance?
A. Early on, there were breaks in our coverage, yes.
Q. Okay. But then, later on it was pretty constant in some form or another?
A. I think that's a fair characterization, yes.
Q. And would you agree that the most prevalent surveillance was a pen register. That was what you used the most to get the biggest swath of time, at least, wouldn't you say?

A. I would have to review the underlying data, but it is possible that either the pen register or search warrants near the end of the case would provide like a large range of data so a search warrant in 2016 that would have logs for that into, you know, all the way into the past.

Q. So when you first started to watch Mr. Danet as a potential suspect in this matter, that was around what date? Let me ask about the period of time this way.

Around what day did you start any surveillance of Mr. Danet in any form?

A. When you say surveillance, are you talking technical surveillance?

Q. I don't mean physical surveillance watching him; I am talking about technical surveillance where you could tell whether he was corresponding with other suspected members of the Bayrob Group.

A. I would estimate in the 2014 range.

Q. Okay. And between 2014 and 2016, Mr. Danet was active that entire time, correct?

MR. BROWN: Objection.

THE COURT: Overruled.

A. Mr. Danet was receiving information — based on the data that I had, I could see that at a minimum Nicolescu was sending information to Danet.

Q. Right. Master Fraud was sending --
A. Yes. Master Fraud was sending data to Danet.
Q. Okay. And in your experience, would there be an operational reason why one member of a criminal enterprise would send information to another if they weren't part of the criminal activity?
A. Can you restate that question?
Q. Here: Mr. Danet said that he took up to four years total or four and-a-half years total off of his activities with the Bayrob Group when he testified the other day.

Do you remember him saying that?

A. I do. Do you have the date ranges for that?
Q. He didn't give any date ranges.

My question for you is: Do you know of any four and-a-half year or any big chunks of time that would add up to four and-a-half years, or was he just lying about that, too?

MR. BROWN: Objection.

THE COURT: Sustained.

BY MR. GOLDBERG:

Q. Do you know about the time frame?
A. I would have to look at the data with that new information to make a determination of whether I could assess that.

Q. Okay. But you did spend sometime parsing out from 2013 forward Mr. Danet's activity as it related to his travels, correct?
A. That's correct, yes.
Q. All right. And you indicated that there was never a log when he was not in Romania, never a log in to — let me be more clear — his criminal e-mail amightysa at GMX —
A. What I stated, when I knew Danet was traveling, I never saw a log or a sent e-mail from that account.
Q. Okay. And that helped lead to the conclusion that Danet was amightysa and not Master Fraud, correct?
A. It did, yes.
Q. And what you used to determine whether or not Danet was traveling were his vacation pictures?
A. Yes, that is correct.
Q. You didn't use any geolocation software or geolocation warrant information, right?
A. No. To be fair to that last question —
Q. Did the pictures contain a location information?
A. So the pictures contained metadata. I was able to look at the pictures and determine where those pictures were taken like where in the world effectively.
So you could see, you know, Danet took a lot of pictures of himself in these pictures, and I could

identify where they were, and then I could also use other data.

So for example, within various like devices — so his phone, for example — he would have reservations for a hotel, for example, in those locations.

So he went to Spain, there would be hotel reservations for that. The photos were like the easiest way to explain it, but there was additional context that was used to essentially establish those things.

Q. All circumstantial evidence of his location?

MR. BROWN: Objection.

THE COURT: Sustained.

A. If you consider a picture of him —

THE COURT: One moment, sir. I sustained it.

THE WITNESS: Oh, I'm sorry.

BY MR. GOLDBERG:

Q. So you didn't have somebody in Morocco that saw him or in Bulgaria that saw him there; you used what was on his phone?

A. What was on his phone and what was on the hard drive containing pictures.

Q. Okay. And no real time GPS, correct?

A. No.

Q. All right. And that's how you determined when he was in the country and when he was out of the country, right?
A. Yes.
Q. And you would agree with me there were three dates on your spreadsheet where he both logged in and was out of the country?
A. Yes, at least. I have looked at the specific time periods, and I was able to see that the travel occurred either before. So if it was a day, for example, where he logged in, there would be an afternoon trip.

So there would be a log-in in the morning, and then he would leave the location and fly to his destination in the afternoon.
Q. But that's not on your spreadsheet that we looked at this morning.

MR. BROWN: Objection.
A. It is in the underlying data.
Q. In the data, not in the exhibit?

MR. BROWN: Objection. It is in the exhibit.

THE COURT: One moment. He can answer that. Overruled.
A. The graph shows what's in the underlying data, so, yes.

Q. The graph, you mean the dots?
A. I'm sorry. It is not clear -- I think I am misunderstanding your question.
Q. Okay. You are saying you had information that he logged in on the same day he was out of the country, that he logged in in the morning or then traveled?
A. Yes, or the reverse, right, where he flew like he was in, let's just say, for example, Turkey and there was a log in that same day, I was able to confirm he came back to Romania and then logged in.
Q. All right. Thank you.
MR. GOLDBERG: Your Honor, may we approach?
THE COURT: Let's do an afternoon recess, and then you can.
Folks. Remember the admonition admonition. All rise for the jury.
(Recess had.)
THE COURT: Please be seated. Mr. Goldberg, you may continue.
MR. GOLDBERG: Thank you, your Honor.
BY MR. GOLDBERG:
Q. Okay. Special Agent Macfarlane, you were shown Exhibit 2203, which is the, the files on the command and control server, correct?
A. That's correct.

Q. Okay.

MR. GOLDBERG: May I approach, your Honor?

THE COURT: You may.

MR. BROWN: Can we pull it up, your Honor?

THE COURT: I'm sorry?

MR. BROWN: Can we display it on the screen?

MR. GOLDBERG: That's fine.

BY MR. GOLDBERG:

Q. Showing you Exhibit 2203 and you said you recognize that correct —

A. Yes.

Q. — and this is information that you yourself took off the command and control server?

A. Yes. This was information that I created for the purpose of this exhibit for — which reflects the data I testified to.

Q. So you didn't take it off the server in this form; you took information —

A. So I mean, if you want — I issued this specific command on this directory, and it provided this tree view of the directory structure.

Q. Okay. And with regard to any — we call these work spaces under Amy, Linux, MF, min, Natiune, Raul, Sasha and TRX, correct?

A. Yes.
Q. And we don't know from your forensic examination of this server who specifically had log-in credentials for the server itself?
A. That is correct.
Q. We have at least one, two, three, four, five, six, seven, eight work spaces, and in each one of those work spaces represents one potential user. Any of those users could have had log-in credentials to work on the command and control server, correct?
A. Yes, if I can clarify.
Q. Is it a yes?
A. It is more complicated than your statement.
Effectively, there were two ways to access the command and control server through secure shell or over the website interface.
Q. Got you. So web interface would be unsecured until it got to the server, and then access the server and secured shell would be secured the whole time?
A. Yes. And to add to that, it would be even more complicated because there were certain pages that were -- that you needed to authenticate to be able to access those pages and certain pages you didn't need to.
Q. But either way, even though you could view all this information on the server, you don't know who was logging

in and working on the server at any particular time?
A. There were certain instances where I could tell which user credentials were being used for certain pages.
Q. Okay. And — but in general, that's not something that you were able to observe in real-time?
A. In real-time? Yes, during my data intercepts, for example, I would see certain pages accessed with certain credentials.
Q. Okay. And were any of those credentials — well, what were the credentials?
A. I can't answer that without the data unfortunately.
Q. Okay. Well, let's just say this: Did the credentials match the monikers that we have discussed here today and throughout this trial?
A. So I can say that I know for sure that I remember seeing Minolta access some of those pages.
Beyond that, I would have a hard time without reviewing the data.
Q. But you can't say that you witnessed the moniker, someone using the moniker Master Fraud or MF accessing the command and control server during your surveillance?

A. It is hard for me to confirm that either way.
Q. During the course of this trial with several witnesses, we saw an array of directional antennas?
A. Yes.
Q. And we saw one directional antenna, and you correct me if I am wrong, and other wireless routers?
A. That's correct.
Q. Were any of those devices forensically inspected for any data they contained or any other trace evidence that would link them to anybody in this case?
I understand they were recovered from certain Defendants' homes, right?
MR. BROWN: Objection.
THE COURT: Sustained.
BY MR. BROWN:
Q. All those devices were seized in certain homes where search warrants were executed?
MR. BROWN: Objection.
THE COURT: Overruled. Is that correct, sir?
A. All the devices were seized from locations listed in the document that contained all the allegations, yes.
Q. Okay. Was there any further forensic evidence gathering done with regard to any of those devices?

A. Not that I am aware of.
Q. Okay. Just to be clear, we don't know a person that may have connected to the internet through any of those devices, an actual human being, correct?
A. Correct.
Q. We don't know any monikers that may have been used through those devices, correct?
A. Correct.
Q. We don't know of any web sessions, internet sessions that were actually conducted through any of those devices?
A. I don't know I can say that for sure. What I do know is that I did see indications on some of the devices that wireless routers were being accessed.
Q. Okay. But again, not relative to any particular person or moniker or IP address?
A. No, that's not true. So, for example -- may I refer to my notes?
Q. Please.
A. Okay. I won't be able to be very specific on this, but we were able to see that there were files related to flashing routers, which is the files that were allowed to basically rewrite the operating system on the routers found on some of the evidence.
Unfortunately, I was not able to say to

which because I don't have those notes with me, and there were also screenshots of -- found on systems belonging to Danet where that would be -- that showed him actually cracking wireless networks.

Q. Nothing relating to Mr. Nicolescu doing that himself but Mr. Danet?

A. That is correct, and there were other data points related to file access found on some of those devices.

Q. But you testified that you were at the search at Mr. Nicolescu's home, correct?

A. That is correct.

Q. Which was actually a house that was rented by Mr. Miclaus, correct?

A. That's correct.

Q. An it was one of his listed addresses, correct?

A. Correct.

Q. And you heard testimony about the devices that were obtained in that search, the digital devices, computers, and hard drives?

A. Correct.

Q. And it is my understanding -- and tell me if I am wrong -- that the computers that were seized from that residence were encrypted?

A. That is correct, yes. There were a number of

encrypted devices or drives.
Q. There was no data available to attribute any of those devices that were encrypted to Mr. Miclaus or Mr. Nicolescu, other than their presence in their shared home?
A. To clarify, the computer devices, that is correct; the phones, that's not correct.
Q. The phones, computer devices?
A. Yes.
Q. Now, am I also correct in stating that there is no digital information that was seized from the computers, from the house where Mr. Nicolescu lived that contained digital evidence connecting him to the Bayrob conspiracy?
A. Can you repeat that one more time?
Q. Yeah, digital evidence contained in any of these computers that were taken out of the house in Brasov that connects Mr. Nicolescu to the command and control servers or any part of the Bayrob Group?
A. All the drives were encrypted.
Q. So the answer is no?
A. Yeah. I can't really tell you what data those drives contain.
Q. The phones that were seized from that house contained information in the form of, at least, a Jabber

account that was similar to the Jabber account on Mr. Danet's phone that was seized in Miami, correct?

A. Yes, the same, I think.

Q. Was it the same exact name, or was it a different server?

A. It was the same user name at a different server.

Q. Different server?

A. Yeah.

Q. And the search occurred in September of '16, and the screenshots and all those conversations taken from Danet's phone occurred up to May 14th --

A. Right around that time.

Q. 2015?

A. Yeah.

Q. So about 14 months later -- 14 months after the Danet seizure was the Nicolescu seizure, correct?

A. You are making me do math again.

Q. September of the next year.

A. Yes.

Q. From May to September of the next year, probably not 14 months. Okay.

When you were able to -- you've indicated you had gone through Mr. Nicolescu's phones, right?

A. Yeah.
Q. And it would be particularly interesting to you what messaging and chat platforms were on his phone, right?
A. Yes.
Q. Did you find WhatsApp on his phone?
A. I would have to review the full report.
Q. All right. Well, I mean, if you found a relevant WhatsApp account because we heard from Mr. Antonovici that he communicated with Mr. Nicolescu, correct?

MR. BROWN: Objection.

THE COURT: Sustained.

BY MR. GOLDBERG:
Q. We heard from Antonovich what he communicated by WhatsApp with Mr. Nicolescu, correct?
A. I don't know. I believe, yeah. I believe that is accurate but —
Q. So it would have made some kind of investigational sense to look to see whether there was even a WhatsApp installed on Mr. Nicolescu's phone, right?
A. Yes.
Q. And as you sit here now, you don't know whether there was or was not?
A. Yeah. I don't know that specific data.

Q. So you made some -- when you were trying to figure out information on who besides Danet was connected to Bayrob, you asked Romania for some information pursuant to an M-LAT request, correct?

You did it many times, but --

A. Yeah. We did M-LAT requests.

Q. And specifically, you asked for requests with Mr. Nicolescu?

A. Yes, that is correct.

Q. And you tried to link him with the name obe among other things?

A. For information on him, yes.

Q. And you got information on the cars he drove, right?

A. Yes.

Q. Where he lives, where he went to school, right?

A. Yes.

Q. Whether he has a criminal record. Did you get that information?

A. I believe we did, yes.

Q. Did he have a criminal record?

MR. BROWN: Objection.

THE COURT: Sustained.

BY MR. GOLDBERG:

Q. Well, if he had a criminal record, would that have

been relevant to your investigation?

MR. BROWN: Objection.

THE COURT: Sustained.

MR. GOLDBERG: Can we see Exhibit 45, please?

BY MR. GOLDBERG:

Q. Exhibit 45 are the Jabber accounts that you were able to extract from the phone you took from Mr. Nicolescu, correct?

A. Correct.

Q. And both obe accounts, obe.m, they both have the same password, correct?

A. They do, yes.

Q. So presumably, if Mr. Danet had the log-ins for his server, then he would have a — he would have the log-ins for both servers because they are the same?

A. I don't know whether he used the same password as this on the server associated with Danet's house.

Q. Because you don't know Danet's server address?

A. No, just because — I don't know. I would have to see another file to be able to tell whether this password was the same.

Q. If I could see Exhibit 23. 23 is whose phone? That's Mr. Nicolescu's phone?

A. Yes.

Q. And there is one obe account on that phone, correct?
A. Yes.
Q. And is there any -- did you find any evidence that Mr. Nicolescu used the moniker obe without the dot m at any time over the Jabber server?
A. Yes.
Q. Where did you find that?
A. On Danet's phone.
Q. What about Mr. Nicolescu's phone?
A. I don't know without looking at the full report.
Q. Well, we can agree then that the address of Mr. Danet's phone was slightly different than the Jabber address on Mr. Nicolescu's phone in Exhibit 23?
A. Yes. That's a different server.
Q. Right. Okay. Can we see Exhibit 227, please? Okay. 227 I believe you identified as a screenshot from Mr. Miclaus' phone, correct?
A. That is correct, yes.
Q. And first of all, we don't have any data information in this phone or any metadata, do we?
MR. BROWN: Object.
BY MR. GOLDBERG:
Q. We don't have any data information in this exhibit

or any metadata?
A. There is no data information in this exhibit, no.
Q. So we have no idea when this was sent, just that it was sent before it was taken off of Mr. Miclaus?
A. No, I don't have the data information for this.
Q. Okay. But we can agree that the address, at least the moniker obe @ aro.strangled.net is different than obe.m @ aro.strangled.net, correct?
A. Yes, you can — those are different.
Q. It is not the same?
A. No. There is the dot m.
Q. And you didn't find any file on Mr. Nicolescu's phone that matched this exact Jabber address, correct?
A. No, but I explained why that would be the case.
MR. GOLDBERG: You can take that down. Thank you. I have nothing further.
THE COURT: Cross examination, Mr. O'Shea?
MR. O'SHEA: Thank you. A moment please, Judge.
THE COURT: Certainly.
(Pause.)
MR. O'SHEA: May I proceed, Judge?
THE COURT: Of course.

CROSS EXAMINATION CONTINUED

BY MR. O'SHEA:

Q. Good afternoon.

A. Good afternoon.

Q. If I heard you correctly, when you first started testifying, you indicated — and you correct me if I am wrong — that you have done hundreds of search warrants in connection with cyber crime. Am I right?

A. Hundreds of search warrants in connection with cyber crime? Absolutely.

Q. Okay. Somewhat prevalent that would necessitate 100 or hundreds of search warrants. Am I right about that agent?

MR. BROWN: Objection.

THE COURT: Sustained.

BY MR. O'SHEA:

Q. Did you do hundreds of search warrants in this case or hundreds of search warrants in your capacity, sir?

A. In my capacity.

Q. Okay. Do you have an idea how many search warrants you did in this case?

A. Roughly 50. That may be an under estimate or overestimate.

Q. Certainly — and you don't certainly have that

number in your notes that you brought with you. Am I right?
A. No.
Q. So 50 out of a hundred as it relates to this case, right?
A. Yes.
Q. Okay. As you sit here right now, sir, do you have any idea why we saw those graphic messages directed to Liam O'Murchu?
MR. BROWN: Objection.
THE COURT: Sustained.
BY MR. O'SHEA:
Q. Could you tell the ladies and gentlemen your experience of what a cookie is, sir?
A. Yes. A cookie is a file that is left on your computer by a website to help that website identify it on the computer.
Q. You heard me ask other witnesses that question. Am I right?
A. I have, yes.
Q. And some of the witnesses in responding to that question, in my opinion, you know, and you can tell me if I am wrong because they didn't like the question, said that some places they asked for your permission before they use cookies, right?

MR. BROWN: Objection.
THE COURT: Sustained.
BY MR. O'SHEA:
Q. Did you hear any witness say when cross-examined on the issue of cookies that some sites tell you when they are placing cookies in there? Did you hear that testimony, sir?
A. Yes, I did.
Q. Would you agree with me that not all sites ask for permission before placing cookies on your computer?
A. It is very location dependent, yes.
Q. So the answer would be yes, right?
A. Depending on where you are, yes.
Q. Okay. And you heard me ask questions about things called PUP. Do you know what a PUP is?
MR. BROWN: Objection.
Q. Potentially a wanted friend. Do you remember Liam O'Murchu talking about that?
THE COURT: Well, now I am going to sustain it. Rephrase your question.
MR. O'SHEA: Sure.
BY MR. O'SHEA:
Q. Do you remember the testimony of Liam O'Murchu?
A. I do, yes.
Q. Okay. Do you remember me asking him questions about

PUP or potentially unwanted programs.
A. Yes. I mean, not specifically, but yes, I remember that portion generally.
Q. And you heard me ask questions of him specifically related to his company about things called adware removable programs, right?
A. Yes.
Q. And that's because adware gets placed on people's computers without their consent, right?
MR. BROWN: Objection.
THE COURT: Sustained.
BY MR. O'SHEA:
Q. Did I hear you say on direct examination that lots of money is moved around to Romania and countries around Romania on a regular basis, sir?
A. In relation to this case?
Q. Cases in general I thought I heard you say.
A. Yeah. I would say that in relation to cyber crime.
Q. Yes, sir.
A. I would say Romania is a place where there is significant movement of money for cyber crime, yes.
Q. Okay. And when you were asked -- I think you told us on direct examination that sometimes when viewing this

thing you call traffic, that most of the time you could not tell where -- who it was coming from or who it was going to.

Did I hear that correctly?

A. You will have to specify your question.

Q. I am just talking about your direct testimony.

A. Okay.

Q. Do you remember saying that?

A. Yes, I would see traffic coming to the command and control server from systems I could identify as infected computers and systems that were acting as relays if that answers your question.

Q. Okay. Let me ask you this: Could you bring up Exhibit 225? That's not one we have seen before.

THE COURT: No.

MR. O'SHEA: I must have the number wrong.

BY MR. O'SHEA:

Q. Let me ask you about this Excel spreadsheet with references to Bayrob?

MR. O'SHEA: One moment, please, Judge.

THE COURT: Sure.

(Pause.)

MR. O'SHEA: Could you put up Exhibit 1137? Let's see if I got that right.

BY MR. O'SHEA:
Q. Do you remember looking at this, testifying about this exhibit, sir?
A. I do, yes.
Q. As I understand it, in layman's terms, this is something that you yourself recreated based upon data that you claimed came from the command and control server. Am I right about that?
MR. BROWN: Objection.
MR. O'SHEA: Let me rephrase the question, Judge.
BY MR. O'SHEA:
Q. Do you recognize Exhibit 1137, sir?
A. I do, yes.
Q. Did you testify previously about this exhibit?
A. I did, yes.
Q. And is this a diagram or a picture that you yourself created?
A. This was a screenshot that I took, yes.
Q. It is a screenshot of a program that is running on Firefox or that you can view on Firefox, that you yourself created in order to kind of mirror traffic of what was going on. Am I right?
A. So what I did here was, I took the data that was on the command and control server and the files that were on

the command and control server, and I recreated that environment, so I could see the files as they interacted with the data.

Q. Okay. So let me take you back just a little bit. Overhead there on that, just so we are clear, 1137 is a document that you yourself as an agent created. Am I right about that, sir?

A. It is a picture of files interacting with the database from the command and control server.

Q. But that document you created. Am I right about that? You didn't find it on anyone's server or a hard drive or phone. Am I right about that?

A. Yeah. I took the picture effectively.

Q. Okay. Can we look at Exhibit 1138? Tell us again what 1138 is, sir.

A. So 1138 is very similar to 1137 in that it is Bayrob, the Bayrob web interface as it talks to the underlying database to present you with a view that would be seen and used by the Bayrob Group.

Q. Did you create this document, sir?

A. I took the picture, yes.

Q. Was this particular picture found on any hard drive or any phone?

A. Yes.

Q. This particular picture, sir?

A. This picture was found on a hard drive when I took a picture and saved the picture. It was on a hard drive. It was not on a command and control server. I needed to create a file of the picture.

Are you talking about like on a specific —

Q. Let me ask you this. Maybe I am confused, and I apologize.

Of all the hard drives that you found during your searches in Romania, was this particular picture found on any of those hard drives?

A. No.

Q. Was this picture found on any of the phones that you seized and searched?

A. No.

Q. If we can go to Exhibit 2201, explain to me in summary real quick what 2201 is again, sir?

A. This is data that was contained within the — one of the tables found in the Bayrob Group database.

Q. Okay. This, correct me if I am wrong, this particular document that we are looking at is sort of like an access or an Excel sheet. Is it not?

A. Yes. It is similar to how data would look in Excel, yes.

Q. Okay. And sometimes in Excel, you actually have

columns and rows like we do here, right?
A. Yeah.
Q. And there are actually lines between them, right?
A. Yes.
Q. And in the context of you during your computer training you have learned how to take data from one document, hit a command, and essentially dump it into an Excel file, right, and have an Excel sheet in front of you just by hitting a few buttons without manually typing.
Am I right about that?
A. Yes.
Q. Now, was this document created that way, or was it manually inputted sir?
A. So this document was created using a tool to access the database and exporting that data out of that database and then displayed in this format.
Q. Okay. Just so I understand you correctly, as relates to Excel, it is not a simple hit of a couple buttons. You actually have to identify how you want the data to be arranged in columns, rows, and that, am I right, sir, when you dump it into one database into another?
A. In this case, no. This was the format it was in.

These were the column names that were in the table, and this was -- I mean this was the data that was in that table.

Q. Let me look at the top of the column. Do you see where it says S-O-X?

A. Yes.

Q. Was that actually the name of the data column in the database it was extracted from?

A. Yes.

Q. Okay. Now, at the top, where it says site 5 Martin Steinberg e-mail list, was that the name of the file on the database?

A. No. Site 5 was the server it came from, and Martin Steinberg's e-mail was a label that I provided.

Q. Okay. So we are clear, the title of this document, which I think appears -- can we go to the next page and the next page, the next page after that?

Okay. Six pages long, at the top of each page, it is the same title, site 5 Martin Steinberg e-mail list. Am I right about that?

A. Yes.

Q. And as part of the program that you are dumping it into, you, the agent, gets to determine what's at the title of each page. Am I right about that?

A. Yes.
Q. And all of the columns -- can we go back to the first page -- all of the columns, SOCKS, e-mail password, status, and use, they were in the original database, or did you create, at least, some of those titles.
A. No, they were in the original data.
Q. But at the top, that title is all donated by you. Is that correct?
A. Yes.
Q. And just so I understand you, to the best of your knowledge, merely storing data is not illegal. Am I right about that?
A. You are correct.
Q. As a matter of fact, Excel is designed to do that very thing. Am I right?
A. Yes. I think that's fair.
Q. Can we go to Exhibit 1204? Same thing, same questions: That's essentially another type of Excel type of program spreadsheet. Am I right about that?
A. Yes.
Q. How about the title to all those columns, who generated that? You or the database it came from?
A. Those were named by the Bayrob Group.
Q. How about the top left-hand corner where it is dream

host, who put that in there?
A. I did. That's where the data came from.
Q. And over here it says CC table?
A. Yes. This was a table, and the name of that table created by the Bayrob Group was CC.
Q. CC table?
A. Just CC.
Q. So CC table, that actual name was created by you. Am I right?
A. That is correct.
Q. Can we go to Exhibit 17? 42. Correct me if I was listening wrong, Special Agent Macfarlane, 1742 is a result of a Google search for the term r-a-d-u-s-p-r?
A. That's incorrect.
Q. What is that?
A. What is this exhibit?
Q. This exhibit ended up -- strike that.
This exhibit caused you after you found it to do a Google search for the term raduspr. Am I right about that?
A. Among others, yes.
Q. And that raduspr, that term was easy to find just used in a Google search, right?
A. There were results from that inquiry, yes.
Q. And something anybody could do from their kitchen or

living room?
A. Yes. Anybody can search that term, yes
Q. Okay. And that type of search is not sophisticated, right?
A. No.
Q. Okay. And that is the search that led you to discover that this term was used, I think, on Twitter and Yahoo, right?
A. Twitter, Facebook. It ended up being a Yahoo account.
Q. Okay. And anybody, be they in Romania, be they in Cleveland, Ohio, that knows this term raduspr could find it and use it on a Twitter, Facebook, or Yahoo account, right?
A. Well, no, they couldn't because it was already reserved. Someone else was already using it.
So they would not be able to use it because it was already used.
Q. Do you have by count at this point how many people have the name Bogdan in this very case alone?
A. I haven't been tracking it, no.
Q. Okay. I see the term Bogdan used for a number of the witnesses and individuals charged and uncharged in this case, right?
MR. BROWN: Object.

THE COURT: Sustained.
BY MR. O'SHEA:
Q. How many times have you been over to Romania?
A. I think five or six.
Q. Did you run over a lot of Bogdans over there, or is it just unusual it comes up so often?
MR. BROWN: Objection.
THE COURT: Sustained.
BY MR. O'SHEA:
Q. When did the — to the best of your understanding from a timeline, when did the cryptoming begin?
A. Based on my recollection, the cryptomining began around the beginning of 2014 would be my best recollection, could have happened a little before that, but 2014 I think is safe.
Q. Could he bring up 1747? Do you remember this document on direct examination?
A. Yes.
Q. And let's see if I can do this. This was a document that you — did you find this document through your Google search?
A. Yes.
Q. Okay. And so easy to find on the internet. Am I right?
A. Yes, that's correct.

Q. And do you see where it is using that name r-a-d-u-s-p-r. Do you see that?
A. I do.
Q. And how many projects has that particular individual or moniker raduspr done according to this exhibit your exhibit, sir?
A. Zero.
Q. Could we bring up Exhibit 367?
THE COURT: Do you want the Elmo?
MR. BROWN: Your Honor, could we have a side bar for a minute?
MR. O'SHEA: All of it? You put up the entire exhibit, and they have already asked about this.
THE COURT: There were only certain pages.
MR. BROWN: Can we have a side bar, your Honor.
THE COURT: You may.
(Side bar held on the record.)
MR. BROWN: We used certain pages and redacted a lot of information.
THE COURT: Right. I don't think you want the whole thing up.
MR. O'SHEA: I just want to ask him how many pages.

THE COURT: Then do it without showing it to the jury.

MR. O'SHEA: That's what I meant, sure.

(Side bar concluded.)

BY MR. O'SHEA:

Q. Agent Macfarlane, do you see —

MR. O'SHEA: By the way, the jury does not see it?

THE COURT: Correct.

BY MR. O'SHEA:

Q. Do you see Exhibit 367?

A. I do now.

Q. Look at the very top there. How many pages is actually Exhibit 367?

A. 734.

Q. Could you scroll down to the last page of the 734-page Exhibit 367? You have to go down here, sir.

Do you see what I am circling right there? Let me just put an arrow right there. Do you see what I have the arrow on on page 734?

A. Yes.

Q. What number is that?

A. 27004.

Q. What does that number reflect, sir?

MR. BROWN: Objection, your Honor.

THE COURT: Let me ask you this: How many messages are in 367, sir?

THE WITNESS: Can you scroll back up to the top, sir?

BY MR. O'SHEA:

Q. Sure. Let me ask you this:

How many lines are there on this exhibit looking at the last page, do you remember? Over 27,000, right?

MR. BROWN: Objection.

THE COURT: Sustained.

BY MR. O'SHEA:

Q. Go to the top of the exhibit, page 1?

MR. BROWN: Objection. Your Honor, could we have a —

THE COURT: Yes.

(Side bar held on the record.)

MR. BROWN: This has translation, so 734 pages is not even — I wouldn't say an equal number of Romanian in English because of formatting and —

THE COURT: Okay. But also, some of this has been redacted.

MR. O'SHEA: Correct.

THE COURT: So you are trying to leave the impression that there is over 700, thousands or whatever,

and the Government isn't showing you everything, and that's really not fair when, in fact, it had to be redacted for you.

Am I wrong on that?

MR. BROWN: We would ask to strike this entire line of questions.

MR. O'SHEA: That's not the reason I ask that it be redacted before. What I am trying to point out is of the 27,000 apparently messages or texts, whatever they are, there are only a few that relate to this case.

That's all I am asking.

THE COURT: That's okay as long as he can include the redacted ones.

MR. O'SHEA: Let me think about that because --

THE COURT: Because then, it is not fair that he is not allowed to mention and include those redacted and the Government has to redact them for you in your client's favor. Am I incorrect?

MR. BROWN: Your Honor, absolutely. I am agreeing wholeheartedly.

MR. O'SHEA: Let me just say this: Let me figure out what we asked to be redacted because all I am trying to ask is -- I am not asking the content; I am

just saying from the number, Judge.

THE COURT: Then you can ask —

MR. BROWN: Your Honor, at this point, having extra time to figure out what he wants to redact or not redact, he has asked the questions. The bell has been rung. We request of you to strike the entire line of questioning.

MR. O'SHEA: I don't understand what the evidentiary basis would be for that, but all I want to ask the witness is — and I am not asking content. The reason we had redaction had to do with content of some of the messages. All I am asking for is number of messages. That's the only point.

THE COURT: But was the content related to this case and redacted?

MR. O'SHEA: No. I will bet a fair majority, the vast majority —

THE COURT: Now, see, the vast majority doesn't help me because now I am hearing yes. Some pertain to this case and were, in fact, redacted. That's the problem I am having with your line of questioning.

So you need to figure out how else to ask it so that we don't get into this redaction business, which isn't fair.

MR. O'SHEA: Again, just so that I can narrow this down, my redaction concerns had to do with the content. All I am asking about the number of messages, that's it.

MR. BROWN: But your Honor, the Government's position is, you can't separate the content from the lines because the content redacted certain lines.

THE COURT: That's my — exactly my concern.

MR. O'SHEA: May I respectfully disagree?

All I am asking is numbers, not content. I am not asking for hearsay; I am not asking what the messages say or anything. I am just asking how many messages total did you have on this particular exhibit. That's it.

THE COURT: Then you have to include those that have been redacted. You must include those in your question, including those that had been redacted for the benefit of —

MR. GOLDBERG: There were some redacted for the benefit of Mr. Nicolescu, and I don't want to just walk in through this door at this moment because I am not waiving my objection to that.

THE COURT: I understand.

MR. O'SHEA: I am going to move along and see —

MR. BROWN: I would move to strike it.
THE COURT: I am not going to strike it. The objection is sustained.
(Side bar concluded.)
BY MR. O'SHEA:
Q. Okay. Let me move on for a moment here, Agent Macfarlane.
I am going to ask you questions about your knowledge about things called directional antennas. Do you remember some of these exhibits that were handed to you on the stand involved hard modems with directional antennas?
A. Yes.
Q. Okay.
A. I think there was just one antenna.
Q. Do you know the different types of directional antennas there are, sir?
A. I know that there are a couple of different types of directional antennae.
Q. Do you know the difference between a short range and long range directional antenna, sir?
A. No.
Q. Just so I am clear, do you know what type of directional antenna that you see was long range or short range? Do you have any idea?

MR. BROWN: Objection.

THE COURT: Overruled. You may answer.

A. I don't have any knowledge on directional, no.

Q. Okay.

MR. O'SHEA: Can we look at Exhibit 1854?

Q. Do you see Exhibit 1854 yet, sir?

A. Not yet.

Q. Do you see it now, sir?

A. I do, yes.

Q. Okay. Is this also an Excel sheet, sir, of sorts?

A. Yes.

Q. Okay. At the very top here, sir —

MR. O'SHEA: Does the jury see it?

THE COURT: Yes.

BY MR. O'SHEA:

Q. At the top, do you see where it says "Master"?

A. Yes.

Q. That's your term. Am I right about that?

A. Yes.

Q. And as it relates to the top of the column, date, time, from, to, subject, attachments, who created those column names?

A. I did.

Q. And am I right this particular exhibit is 114 pages

long?

MR. BROWN: Objection, your Honor.

Q. Do you see that?

THE COURT: Based on the same conversation.

MR. BROWN: Yes, your Honor.

THE COURT: Sustained.

BY MR. O'SHEA:

Q. Do you see the bottom left-hand corner of Exhibit 1854, sir?

A. I do, yes.

Q. Now, this content came from where?

A. This content came from e-mail service providers that we served legal process on.

Q. Okay. Which one?

A. GMX, and I would have to see the rest of the sheet to be able to tell you the other providers but generally GMX, AOL, and gmail.

Q. And did you manually type yourself in as opposed to dump in from database say from database A to database B? Did you manually type in these items?

A. I did not, no.

Q. How did they get them?

A. I pulled them from the data that was provided and put them into this document.

Q. Okay. But did you have to manually put them into

the program?
A. No.
Q. What technique did you use to get this data into Exhibit 1854?
A. Specifically, I don't recall what technique I used.
Q. But so that we are clear, unlike the other Excel sheets, this is not from a database; this is an Excel worksheet that you created, either manually inputting it or dumping the data in from somewhere else. Am I right about that?
A. Yes.
Q. Now, one of the things I heard you say on direct examination — and correct me if I am wrong — at some point, we indicted the Defendants. Do you remember saying that on direct examination, sir?
A. Yes.
Q. Isn't it true that you did not indict anybody; that it was another body, not you, you can't indict anybody, can you?
MR. BROWN: Objection, your Honor.
THE COURT: Overruled, yeah. Maybe it was bad wording.
BY MR. O'SHEA:
Q. Okay. A number of the times during your testimony,

sir, I noted that you had to use notes to refresh your recollection. Am I right about that?
A. You are correct about that.
Q. Okay. Why?
A. Because this was a long and data intentive case.
Q. And it involved an alarming amount of data and information. Would I be right about that, sir?
A. You would be correct.
Q. Could we look at Exhibit 1849? One moment, please.
THE COURT: Certainly.
(Pause.)
BY MR. O'SHEA:
Q. Now, what we are watching — can the jury see this?
THE COURT: Yes.
Q. Right now what we saw before I start the question, one had to actually tap on a file and launch an Excel program, the same program I was talking about before on Excel in or to view this data. Am I right about that, sir?
A. That is correct.
Q. Okay. And Excel is one of those programs that I was just asking you questions about before, right, sir?
A. That is correct.
Q. All right. And Excel is, in fact, the program that

you've used to create some of these exhibits. Am I right about that, sir?
A. That is correct.
Q. Okay. Now, the data in this program — could we go all the way to the top of that exhibit, 1849? All right.
We see here date, amighty, amighty, PRTT log-in data, Master Fraud, Danet travel, all of those titles to all of those columns were created by you. Am I right about that, sir?
A. Yes.
Q. How did this data get in here? Was it manually inputted by you, or was it dumped in there through some sort of, you know, comma separated value or tab separated value, file transfer?
A. Yes. It was imported from whatever the original format was.
Q. Okay. Did I see on one of these Excel sheets that was produced in this case where you actually had an Excel column titled "cookies"?
MR. BROWN: Objection.
THE COURT: Sustained.
BY MR. O'SHEA:
Q. Did you in the course of your investigation create an Excel file, the title of one of the columns being "cookies"?

MR. BROWN: Objection.
THE COURT: Sustained.
BY MR. O'SHEA:
Q. Now, Detective, if I understand you correctly, were you in Romania on the day that the arrest and search warrants executions took place?
A. I was, yes.
Q. Okay. How many people were in, if any, other than Mr. Danet, Mr. Danet's home?
A. I don't know. I was not at Danet's house.
Q. How about Mr. Nicolescu, how many people were at his house?
A. I would estimate roughly between eight and 12 maybe.
Q. How many of them were agents?
A. I believe I was the only one there.
Q. How many of them were authorities as opposed to non authorities?
MR. BROWN: Objection.
BY MR. O'SHEA:
Q. By that, I mean agents, Romanian police, FBI agents, how many were layman to ask it another way?
MR. BROWN: Objection.
THE COURT: Overruled. Can you answer?
THE WITNESS: I can't.

BY MR. O'SHEA:
Q. Other than Mr. Nicolescu, who else was in his apartment before the authorities went in. Let me ask that.
MR. BROWN: Objection.
THE COURT: Sustained.
BY MR. O'SHEA:
Q. Do you know how many people that were not agents or authorities of any governmental entity that were in that apartment that day?
MR. BROWN: Objection.
THE COURT: Overruled. Do you know, sir?
THE WITNESS: Can you restate that question?
BY MR. O'SHEA:
Q. Take yourself back to Mr. Nicolescu's apartment. Place yourself in that apartment.
I think you said there were about ten or 12 people total in the apartment?
A. I think I said between eight and 12 people.
Q. And of those eight or 12 people, how many were people that would have shields or credentials of any governmental agency?
MR. BROWN: Objection.
THE COURT: Overruled. Do you know, sir?
A. Yeah. I don't know.

Q. Half?

MR. BROWN: Objection.

Q. In an attempt to refresh your recollection, sir —

THE COURT: Overruled.

BY MR. O'SHEA:

Q. Like you have done with your notes, let me suggest half.

A. I don't — I just don't know.

Q. Were you there, sir, when they went into the apartment?

A. I was, yes.

Q. And were there other apartments in the complex?

MR. BROWN: Objection.

THE COURT: Overruled.

A. It was a house.

Q. Were there other people around, other houses?

A. Yes. There were other houses.

Q. And when those officers went in, were there people standing on the street watching this happen? Do you remember?

A. No.

Q. Was anyone allowed to use a telephone that day?

A. I don't know.

Q. How about going to the home of Mr. Miclaus or the residences you searched relative to Mr. Miclaus? Were you there for any of those?
A. I was not, no.
Q. All you were there for was Bogdan Nicolescu?
A. That is correct.
Q. And you can't remember, as you sit here today, of the people that were in that apartment were non agents? Is that what you are telling me?
A. I don't know that I even knew that from the beginning. I didn't say I can't remember. I have just said I don't know.
Q. What's the difference between I can't remember and I don't know?
MR. BROWN: Objection.
THE COURT: Sustained.
BY MR. O'SHEA:
Q. You don't remember?
A. No.
Q. And as you sit here now, of the eight to 10 people, you don't know how many of them were agents?
MR. BROWN: Objection.
A. That is correct, yes.
Q. Were you ever present, sir, when the lot of them were taken down to the Romanian Police Department or

police station?
A. Yes. I was at the location they were taken to.
Q. How many people were taken to the location other than the two Defendants?
A. I observed approximately five to six people.
Q. In addition to the Defendants. Am I right?
A. No, not in addition to the Defendants.
Q. Including the Defendants?
A. Including the Defendants.
Q. Can we look at Exhibit 45? Do you remember testifying about Exhibit 45 on direct examination, sir?
A. Yes, I do.
Q. Am I right that you had not once but twice had to refer to your notes to confirm exactly what this was. Did I see that correctly?
A. That is right.
Q. Could you have been able to do it without your notes?

MR. BROWN: Objection.

THE COURT: Sustained.

BY MR. O'SHEA:
Q. Could we go to Exhibit 23? Same question: Am I right that you had to use your notes to remember what this was?

A. To remember where it was from?
Q. When you were asked a question by Mr. Goldberg, I think you had to use — or I'm sorry. Mr. Brown — you had to use your notes to refresh your recollection. Am I right about that?
A. Yes.
Q. Could we look at Exhibit 232? What is Exhibit 232 again?
A. Exhibit 232 is the data contained in the accounts table from the Xabber database found on this phone.
Q. On whose phone?
A. Miclaus phone.
Q. Let me ask you this in layman's terms or police terms: Tell the ladies and gentlemen of the jury what a phone dump is?
A. You are talking about a forensic image as a phone?
Q. Or sometimes referred to as a phoneup. You heard that before?
A. Yes.
Q. So sort of like — and you seize a phone that you can take and dump all the data out of it, right?
A. Yes.
Q. And sometimes it is an enormous amount of data. Am I right about that?

A. Yes.
Q. Thousands of pages?
A. Yes.
Q. And it is not unusual, even if you were talking about my 21 year-old daughter or anyone else, there is usually an enormous amount of data in one cellphone?
A. Yes.
Q. One said the cellphone is more sophisticated than the lunar module we had go to the moon. Am I right about that?

MR. BROWN: Objection.

THE COURT: Sustained.

BY MR. O'SHEA:
Q. This what we see on Exhibit 232, that's not the entirety of the data on the phone. Am I right?

MR. BROWN: Objection.

THE COURT: Overruled. You may answer.

A. You are correct.
Q. Now, staying with 232, if I am not mistaken, sir, does this exhibit actually give us the content of any messages?
A. No. It does not.
Q. Can we look at Exhibit 227? Do you remember testifying about this exhibit on direct examination, sir?

A. Yes, sir.
Q. All right. If I understood one of the questions that was asked of you, either on direct examination or cross examination, is that you don't have a date for this chat. Am I right about that?
A. That is correct.
Q. Okay. Do you remember being shown sessions of the indictment that had tables in them, sir?
A. I do, yes.
Q. Okay. Just so that we are clear, just like that Excel sheet that we talked about before, the columns and the data in those tables were created my you, right?
A. Yes.
Q. Do you remember being shown that other table about cryptomining. Do you remember that?
A. Yes.
Q. That table, same question.
A. Same answer.
MR. BROWN: Objection, your Honor. Can't ask questions like that.
THE COURT: Sustained.
BY MR. O'SHEA:
Q. Let me ask you this: Do you remember being shown a table with domain names on it on direct examination,

sir?
A. I do.
Q. That table was created entirely by you, right?
A. The table was created by me, yes.
MR. O'SHEA: One moment, please, Judge.
THE COURT: Sure.
(Pause.)
MR. O'SHEA: Can I still have a moment, Judge?
THE COURT: Certainly.
(Pause.)
BY MR. O'SHEA:
Q. One last question, sir: Until any of the exhibits that we have seen through your testimony where the term "Bayrob" is used, can we assume, sir, that term, if seen in the exhibit, was placed in there my law enforcement and/or others; not the people in this -- at these two tables here. Am I right about that?
MR. BROWN: Objection.
THE COURT: Overruled. You may answer.
A. I would say -- I have seen a lot of exhibits, so my apologies for not being able to remember all of them.
Q. Okay.
A. I would say generally that is true. There may be

some -- there was e-mail between the group that contained Bayrob in it.
Q. The term "Bayrob"?
A. The term "Bayrob", yes.
Q. So at some point, is it your belief that the evidence shows that these folks were aware that they were called Bayrob?
A. Yes. The investigation definitely revealed that they were aware that they were called Bayrob because they were following the investigation done by Liam O'Murchu and actually input into the malware his information and thoughts, which suggests to me that they were well aware they were called Bayrob.
Q. All right. Well, whoever for purposes of my question, Bayrob what? There was the term Bayrob I think we got from Liam O'Murchu, was a term that he created as far back as 2009, am I right about that, when he started writing and blogging about it?
A. Approximately back then, give or take a few years.
Q. Absent any e-mails or texts that use that term, if the title of any exhibit at the top uses the term "Bayrob," could we assume that law enforcement put that at the top of that exhibit and not anybody that might have been in that group, sir?
A. Definitely, I think that probably is correct. I

would have to review all the exhibits so make sure that is correct.

Q. And nothing in the notes that you have in front of you would be able to assist you in refreshing your recollection in order to answer that question. Is that right?

A. That's correct.

MR. O'SHEA: One moment please, Judge.

(Pause).

MR. O'SHEA: Nothing further.

THE COURT: Any redirect?

MR. BROWN: No, your Honor.

THE COURT: You may step down, sir.

Folks, we will adjourn for the evening. Please be downstairs at 9:00 a.m. We will call for you at that time.

Do not form any opinion regarding this case. Do not talk about it. We will see you tomorrow morning at 9:00 a.m. Have a good evening, folks.

(Jury out.)

MR. GOLDBERG: I have an issue and doesn't need to be on the record.

THE COURT: Off the record, George.

(Discussion held off the record.)

THE COURT: Are we ready to go on the

record?

MR. GOLDBERG: Ready, Judge?

THE COURT: 1204, 1755.

MR. GOLDBERG: Can we have them come up?

MR. O'SHEA: Ours aren't coming up, Judge.

THE COURT: Oh. Sue, can we go — let's go back. 1204 and again, I am assuming you are offering it unless the Government, you tell me otherwise?

MR. BROWN: Correct, your Honor.

THE COURT: I assume no objection unless you tell me. Or if you previously objected, I will take note and say it. So 1204 is our first one. 1755, I believe Defendant Miclaus objected.

Are you maintaining your objection, Mr. O'Shea?

MR. O'SHEA: I am thinking, Judge.

THE COURT: I just wanted to make sure you knew I was referring to you.

MR. O'SHEA: Maintaining my objection, Judge.

THE COURT: It is allowed over Defendant Miclaus' objection.

1750, Government, correct me, if I am wrong, it is page 1 only. Am I correct?

MR. BROWN: Yes. Correct, your Honor.

THE COURT: 1747, my understanding both Defendants objected.

Mr. Goldberg, are you maintaining your objection?

MR. GOLDBERG: I am, your Honor. This was found, testified by the witness open source. It doesn't — the only attribution for it is raduspr, the name raduspr. There was no data regarding who posted this or anything to either directly link it to Mr. Nicolescu. It is just something the agent got off the internet, and I don't think it is probative enough.

THE COURT: Mr. O'Shea?

MR. O'SHEA: And if this comes in, then any document that any agent finds on the internet and says I found it on the internet is admissible.

MR. BROWN: We are pulling this up right now, your Honor, but this is the subject of page 25 of the authentication motion, which was granted by the Court.

THE COURT: I didn't hear that last part.

MR. BROWN: I'm sorry. It was argued in the authentication motion, and this was ruled on and granted by the Court.

THE COURT: I don't think they are objecting on authentication grounds.

MR. BROWN: I think Mr. O'Shea did.

THE COURT: Well, I thought it was — maybe I misunderstood you, Mr. O'Shea.

Mr. Goldberg, are you objecting on authentication grounds.

MR. GOLDBERG: No. I know it was preauthenticated. I know it is what the agent took off the internet.

I think it is way more — it purports to prove a lot more —

THE COURT: Relevancy is what I took your objection.

MR. GOLDBERG: Relevancy and undue presence.

MR. BROWN: I think the testimony that was not objected to was about the name that was used on this page, but the relevancy was supported by the fact it was authentic; that it was done as part of a larger search, as part of the larger investigation.

The witness testified to why he thought it was reliable or more probable that it was the Defendants based on the nickname, the skill set, and the location.

THE COURT: I am going to allow it over the objection of both Defendants.

Exhibit 367, Government, correct me if I am wrong, pages 714, 715, 716, 717, 722, and 176.

MR. BROWN: You are throwing a curve ball with 176.

THE COURT: I thought I made a mistake there.

MR. BROWN: And the 714 and the 722, if I remember correctly, were subject to redaction. If I am wrong on those pages, it would be subject to appropriate action.

MR. O'SHEA: No objection to that with the redactions, Judge.

THE COURT: With the redactions?

MR. O'SHEA: And the jury will know that it is only limited pages.

THE COURT: All right.

MR. BROWN: Okay. But your Honor — and I have been also corrected by Ms. Chandler — that when Danet testified, he testified to page 718, 732, 733, and 734. That's why she is the best, your Honor.

THE COURT: You are not kidding.

718, 732, 733, 734, you are absolutely correct.

Mr. O'Shea?

MR. O'SHEA: No objection.

THE COURT: Mr. Goldberg?

MR. GOLDBERG: No objection.

THE COURT: All right. 1886, 2069, 1854, Government, you are not offering 1849, or am I incorrect?

MR. BROWN: I'm sorry. I was having a side conversation.

THE COURT: 1849, is that demonstrative?

MR. BROWN: Oh, correct. That's demonstrative.

THE COURT: Or are you offering it?

MR. O'SHEA: Was that the timeline?

MR. BROWN: We will offer it just as a demonstrative, your Honor.

THE COURT: Well, then, you are not offering it into evidence?

MR. BROWN: Correct, your Honor, just using it as a demonstrative.

THE COURT: You are using it as a demonstrative.

So it is not offered and not going to the jury.

45, 23, 185.

MR. LEVINE: Physical exhibit.

MR. BROWN: It is the phone.

THE COURT: The 185?

MR. BROWN: Yes.

MR. GOLDBERG: What is it?

MR. BROWN: It is the phone.

THE COURT: The phone. 232, 227, 2203. On behalf of the Government, did I miss anything?

MR. BROWN: Your Honor, let me check with my expert.

(Pause.)

MR. BROWN: Your Honor, I have permission from Ms. Chandler to say the Government thinks we have everything.

MR. GOLDBERG: Nothing on behalf of the Mr. Nicolescu.

MR. O'SHEA: Nothing further, Judge.

THE COURT: All right.

MR. O'SHEA: I don't have any objection.

THE COURT: We are in adjournment. See everyone tomorrow morning.

MR. BROWN: Thank you, your Honor.

(Trial adjourned at 4:50 p.m.)

- - - - -

C E R T I F I C A T E

I, George J. Staiduhar, Official Court Reporter do hereby certify that the foregoing is a true and correct transcript of the proceedings herein.

s/George J. Staiduhar